NSA Core Intelligence Oversight Training:

1. (U) Executive Order (E.O.) 12333, as amended United States Intelligence Activities
2. (U//FOUO) Procedures 1-4, 14, and 15 of DoD 5240.1-R, "Procedures for Department of Defense Intelligence Components That Affect US Persons"
3. (U//FOUO) Directive Type Memorandum (DTM-08-052), "DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters"
4. (S//SI) NSA/CSS Policy 1-23, Procedures governing activities of NSA/CSS that affect US Persons

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20350901

NSA Core Intelligence Oversight Training:

1. (U) Executive Order (E.O.) 12333, as amended United States Intelligence Activities
2. (U/~~/FOUO)~~ Procedures 1-4, 14, and 15 of DoD 5240.1-R, "Procedures for Department of Defense Intelligence Components That Affect US Persons"
3. (U/~~/FOUO)~~ Directive Type Memorandum (DTM-08-052), "DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters"
4. ~~(S//SI)~~ NSA/CSS Policy 1-23, Procedures governing activities of NSA/CSS that affect US Persons

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20350901

EXECUTIVE ORDER
12333

\- - - - - - - -

UNITED STATES INTELLIGENCE ACTIVITIES

DECEMBER 4, 1981

(AS AMENDED BY EXECUTIVE ORDERS 13284 (2003), 13355 (2004) AND 13470 (2008))

PREAMBLE

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended, (Act) and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1 *Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts*

1.1 *Goals.* The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its

interests.

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:

(1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;

(2) Threats to the United States and its interests from terrorism; and

(3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector

entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 *The National Security Council.*

(a) *Purpose.* The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) *Covert Action and Other Sensitive Intelligence Operations.* The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 *Director of National Intelligence.* Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence

Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

(1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

(2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

(1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source

derived;

(2) May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;

(3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

(4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

(A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

(B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

(C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

(5) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:

(A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:

(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

(10) May, only with respect to Intelligence Community elements, and after consultation with the head of the

originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National

Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.

(B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;

(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities

for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish

procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of

Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;

(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed

intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for

Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) Removal from certain positions.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State

for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

1.4 *The Intelligence Community.* Consistent with applicable Federal law and with the other provisions of this order, and

under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;

(g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 *Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies.* The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request,

after consultation with the head of the department or agency, for the performance of the Director's functions;

(e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of

combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

1.6 *Heads of Elements of the Intelligence Community.* The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;

(f) Disseminate information or intelligence to foreign

governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 *Intelligence Community Elements.* Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

(a) THE CENTRAL INTELLIGENCE AGENCY. The Director of the Central Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;

(2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for

cover and proprietary arrangements;

(4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;

(2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;

(3) Conduct counterintelligence activities;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;

(6) Manage and coordinate all matters related to the Defense Attaché system; and

(7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the

direct support of military commanders;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;

(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with

sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and

(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international

organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.8 *The Department of State*. In addition to the authorities

exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:

(a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;

(b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

(c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and

(d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 *The Department of the Treasury.* In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 *The Department of Defense.* The Secretary of Defense shall:

(a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;

(b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill

national, departmental, and tactical intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in sections (a) though (i) above, and to support the Intelligence Community elements of the Department of

Defense; and

(k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense,

(h) above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 *The Department of Homeland Security.* In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 *The Department of Energy.* In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;

(b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 *The Federal Bureau of Investigation.* In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

PART 2 *Conduct of Intelligence Activities*

2.1 *Need.* Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 *Purpose.* This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction,

and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 *Collection of information.* Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign

intelligence, counterintelligence, international drug or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the

Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 *Collection Techniques.* Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession;

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a non-intelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 *Attorney General Approval.* The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 *Assistance to Law Enforcement and other Civil Authorities.* Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;

(b) Unless otherwise precluded by law or this Order,

participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 *Contracting.* Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 *Consistency With Other Laws.* Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 *Undisclosed Participation in Organizations Within the United States.* No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by

the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 *Human Experimentation.* No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 *Prohibition on Assassination.* No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

2.12 *Indirect Participation.* No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 *Limitation on Covert Action.* No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 *General Provisions*

3.1 *Congressional Oversight.* The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall

be implemented in accordance with applicable law, including title V of the Act. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 *Implementation.* The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

3.3 *Procedures.* The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 *References and Transition.* References to "Senior Officials of the Intelligence Community" or "SOICs" in executive orders or

other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 *Definitions.* For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) *Covert action* means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) Activities to provide routine support to the overt activities (other than activities described in

paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(c) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Employee* means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) *Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) *Intelligence* includes foreign intelligence and counterintelligence.

(g) *Intelligence activities* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) *Intelligence Community* and elements of the Intelligence Community refers to:

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) The other offices within the Department

of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) *National Intelligence and Intelligence Related to National Security* means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its

people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(j) *The National Intelligence Program* means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) *United States person* means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 *Revocation*. Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

3.7 *General Provisions*.

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

(1) Authority granted by law to a department or agency, or the head thereof; or

(2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

/s/ Ronald Reagan

THE WHITE HOUSE

December 4, 1981

DoD 5240 1-R

DEPARTMENT OF DEFENSE

PROCEDURES GOVERNING THE

ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS

DECEMBER 1982

UNDER SECRETARY OF DEFENSE FOR POLICY

FOREWORD

This DoD regulation sets forth procedures governing the activities of DoD intelligence components that affect United States persons. It implements DoD Directive 5240.1, and replaces the November 30, 1979 version of DoD Regulation 5240.1-R. It is applicable to all DoD intelligence components.

Executive Order 12333, "United States Intelligence Activities," stipulates that certain activities of intelligence components that affect U.S. persons be governed by procedures issued by the agency head and approved by the Attorney General. Specifically, procedures 1 through 10, as well as Appendix A, herein, require approval by the Attorney General. Procedures 11 through 15, while not requiring approval by the Attorney General, contain further guidance to DoD Components in implementing Executive Order 12333 as well as Executive Order 12334, "President's Intelligence Oversight Board".

Accordingly, by this memorandum, these procedures are approved for use within the Department of Defense. Heads of DoD components shall issue such implementing instructions as may be necessary for the conduct of authorized functions in a manner consistent with the procedures set forth herein.

This regulation is effective immediately.

William French Smith 10/4/82
Attorney General of the United States

Caspar W. Weinberger 12/7/82
Secretary of Defense

TABLE OF CONTENTS

TABLE OF CONTENTS, continued

TABLE OF CONTENTS, continued

REFERENCES

(a) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(b) Public Law 95-511, "Foreign Intelligence Surveillance Act of 1978"
(c) DoD Directive 5200.29, "DoD Technical Surveillance Countermeasures (TSCM) Survey Program," February 12, 1975
(d) Chapters 105 and 119 of title 18, United States Code
(e) Public Law 73-416, "Communications Act of 1934," Section 605
(f) Sections 801-840 of title 10, United States Code, "Uniform Code of Military Justice"
(g) Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979
(h) Executive Order 12198, "Prescribing Amendments to the Manual for Courts-Martial, United States, 1969," March 12, 1980
(i) DoD Directive 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," March 22, 1982
(j) DoD Directive 5000.11, "Data Elements and Data Codes Standardization Program," December 7, 1964
(k) DoD Directive 5000.19, "Policies for the Management and Control of Information Requirements," March 12, 1976

DL1. DEFINITIONS

DL1.1.1. Administrative Purposes. Information is collected for "administrative purposes" when it is necessary for the administration of the component concerned, but is not collected directly in performance of the intelligence activities assigned such component. Examples include information relating to the past performance of potential contractors; information to enable such components to discharge their public affairs and legislative duties, including the maintenance of correspondence files; the maintenance of employee personnel and training records; and training materials or documents produced at training facilities.

DL1.1.2. Available Publicly. Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public. In this context, the "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

DL1.1.3. Communications Security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such telecommunications.

DL1.1.4. Consent. The agreement by a person or organization to permit DoD intelligence components to take particular actions that affect the person or organization. Consent may be oral or written unless a specific form of consent is required by a particular procedure. Consent may be implied if adequate notice is provided that a particular action (such as entering a building) carries with it the presumption of consent to an accompanying action (such as search of briefcases). (Questions regarding what is adequate notice in particular circumstances should be referred to the legal office responsible for advising the DoD intelligence component concerned.)

DL1.1.5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

DL1.1.6. <u>Counterintelligence Investigation</u>. Includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other intelligence activities, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

DL1.1.7. <u>DoD Component</u>. Includes the Office of the Secretary of Defense, each of the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies.

DL1.1.8. <u>DoD Intelligence Components</u>. Include the following organizations:

DL1.1.8.1. The National Security Agency/Central Security Service.

DL1.1.8.2. The Defense Intelligence Agency.

DL1.1.8.3. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.

DL1.1.8.4. The Assistant Chief of Staff for Intelligence, Army General Staff.

DL1.1.8.5. The Office of Naval Intelligence.

DL1.1.8.6. The Assistant Chief of Staff, Intelligence, U. S. Air Force.

DL1.1.8.7. The Army Intelligence and Security Command.

DL1.1.8.8. The Naval Intelligence Command.

DL1.1.8.9. The Naval Security Group Command.

DL1.1.8.10. The Director of Intelligence, U.S. Marine Corps.

DL1.1.8.11. The Air Force Intelligence Service.

DL1.1.8.12. The Electronic Security Command, U.S. Air Force.

DL1.1.8.13. The counterintelligence elements of the Naval Investigative Service.

DL1.1.8.14. The counterintelligence elements of the Air Force Office of Special Investigations.

DL1.1.8.15. The 650th Military Intelligence Group, SHAPE.

DL1.1.8.16. Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E.O. 12333 (reference (a)), applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation.

DL1.1.9. Electronic Surveillance. Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b)).)

DL1.1.10. Employee. A person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency.

DL1.1.11. Foreign Intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

DL1.1.12. Foreign Power. Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities.

DL1.1.13. Intelligence Activities. Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333 (reference (a)).

DL1.1.14. Intelligence Community and an Agency of Or Within the Intelligence Community. Refers to the following organizations:

DL1.1.14.1. The Central Intelligence Agency (CIA).

DL1.1.14.2. The National Security Agency (NSA).

DL1.1.14.3. The Defense Intelligence Agency (DIA).

DL1.1.14.4. The Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.

DL1.1.14.5. The Bureau of Intelligence and Research of the Department of State.

DL1.1.14.6. The intelligence elements of the Army, the Navy, the Air Force and the Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy.

DL1.1.14.7. The staff elements of the Office of the Director of Central Intelligence.

DL1.1.15. International Narcotics Activities. Refers to activities outside the United States to produce, transfer or sell narcotics or other substances controlled in accordance with Sections 811 and 812 of title 21, United States Code.

DL1.1.16. International Terrorist Activities. Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

DL1.1.17. Lawful Investigation. An investigation qualifies as a lawful investigation if the subject of the investigation is within DoD investigative jurisdiction; if it is conducted by a DoD Component that has authorization to conduct the particular type of investigation concerned (for example, counterintelligence, personnel security, physical security, communications security); and if the investigation is conducted in accordance with applicable law and policy, including E.O. 12333 and this Regulation.

DL1.1.18. Personnel Security. Measures designed to insure that persons employed, or being considered for employment, in sensitive positions of trust are suitable for such employment with respect to loyalty, character, emotional stability, and reliability and that such employment is clearly consistent with the interests of the national security. It includes measures designed to ensure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security.

DL1.1.19. Personnel Security Investigation:

DL1.1.19.1. An inquiry into the activities of a person granted access to intelligence or other classified information; or a person who is being considered for access to intelligence or other classified information, including persons who are granted or may be granted access to facilities of DoD intelligence components; or a person to be assigned or retained in a position with sensitive duties.emsp; The investigation is designed to develop information pertaining to the suitability, eligibility, and trustworthiness of the individual with respect to loyalty, character, emotional stability and reliability.

DL1.1.19.2. Inquiries and other activities directed against DoD employees or members of a Military Service to determine the facts of possible voluntary or involuntary compromise of classified information by them.

DL1.1.19.3. The collection of information about or from military personnel in the course of tactical training exercises for security training purposes.

DL1.1.20. Physical Security. The physical measures taken to prevent unauthorized access to, and prevent the damage or loss of, equipment, facilities, materiel and documents; and measures undertaken to protect DoD personnel from physical threats to their safety.

DL1.1.21. Physical Security Investigation. All inquiries, inspections, or surveys of the effectiveness of controls and procedures designed to provide physical security; and all inquiries and other actions undertaken to obtain information pertaining to physical threats to DoD personnel or property.

DL1.1.22. Reasonable Belief. A reasonable belief arises when the facts and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not.

DL1.1.23. Signals Intelligence. A category of intelligence including communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combination.

DL1.1.24. United States. When used to describe a place, the term shall include the territories under the sovereignty of the United States.

DL1.1.25. United States Person

DL1.1.25.1. The term "United States person" means:

DL1.1.25.1.1. A United States citizen;

DL1.1.25.1.2. An alien known by the DoD intelligence component concerned to be a permanent resident alien;

DL1.1.25.1.3. An unincorporated association substantially composed of United States citizens or permanent resident aliens;

DL1.1.25.1.4. A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person.

DL1.1.25.2. A person or organization outside the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained. An alien in the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained.

DL1.1.25.3. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.

C1. CHAPTER 1

PROCEDURE 1. GENERAL PROVISIONS

C1.1. APPLICABILITY AND SCOPE

C1.1.1. These procedures apply only to "DoD intelligence components," as defined in the Definitions Section. Procedures 2 through 4 provide the sole authority by which such components may collect, retain and disseminate information concerning United States persons. Procedures 5 through 10 set forth applicable guidance with respect to the use of certain collection techniques to obtain information for foreign intelligence and counterintelligence purposes. Authority to employ such techniques shall be limited to that necessary to perform functions assigned the DoD intelligence component concerned. Procedures 11 through 15 govern other aspects of DoD intelligence activities, including the oversight of such activities.

C1.1.2. The functions of DoD intelligence components not specifically addressed herein shall be carried out in accordance with applicable policy and procedure.

C1.1.3. These procedures do not apply to law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components. When an investigation or inquiry undertaken pursuant to these procedures establishes reasonable belief that a crime has been committed, the DoD intelligence component concerned shall refer the matter to the appropriate law enforcement agency in accordance with procedures 12 and 15 or, if the DoD intelligence component is otherwise authorized to conduct law enforcement activities, shall continue such investigation under appropriate law enforcement procedures.

C1.1.4. DoD intelligence components shall not request any person or entity to undertake any activity forbidden by Executive Order 12333 (reference (a)).

C1.2. PURPOSE

The purpose of these procedures is to enable DoD intelligence components to carry out effectively their authorized functions while ensuring their activities that affect U.S. persons are carried out in a manner that protects the constitutional rights and privacy of such persons.

C1.3. INTERPRETATION

C1.3.1. These procedures shall be interpreted in accordance with their stated purpose.

C1.3.2. All defined terms appear in the Definitions Section. Additional terms, not otherwise defined, are explained in the text of each procedure, as appropriate.

C1.3.3. All questions of interpretation shall be referred to the legal office responsible for advising the DoD intelligence component concerned. Questions that cannot be resolved in this manner shall be referred to the General Counsel of the Military Department concerned, or, as appropriate, the General Counsel of the Department of Defense for resolution.

C1.4. EXCEPTIONS TO POLICY

Requests for exception to the policies and procedures established herein shall be made in writing to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense and, if required, the Attorney General for any such exception.

C1.5. AMENDMENT

Requests for amendment of these procedures shall be made to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense, and, if required, the Attorney General, for any such amendment.

C2. CHAPTER 2

PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS

C2.1. APPLICABILITY AND SCOPE

This procedure specifies the kinds of information about United States persons that may be collected by DoD intelligence components and sets forth general criteria governing the means used to collect such information. Additional limitations are imposed in Procedures 5 through 10 on the use of specific collection techniques.

C2.2. EXPLANATION OF UNDEFINED TERMS

C2.2.1. Collection. Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

C2.2.2. Cooperating sources means persons or organizations that knowingly and voluntarily provide information to DoD intelligence components, or access to information, at the request of such components or on their own initiative. These include Government Agencies, law enforcement authorities, credit agencies, academic institutions, employers, and foreign governments.

C2.2.3. Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization, or person.

C2.2.4. Overt means refers to methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that he is providing such information to the Department of Defense or a component thereof.

C2.3. <u>TYPES OF INFORMATION THAT MAY BE COLLECTED ABOUT UNITED STATES PERSONS</u>

Information that identifies a United States person may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component, and only if it falls within one of the following categories:

C2.3.1. <u>Information Obtained With Consent</u>. Information may be collected about a United States person who consents to such collection.

C2.3.2. <u>Publicly Available Information</u>. Information may be collected about a United States person if it is publicly available.

C2.3.3. <u>Foreign Intelligence</u>. Subject to the special limitation contained in section C2.5., below, information may be collected about a United States person if the information constitutes foreign intelligence, provided the intentional collection of foreign intelligence about United States persons shall be limited to persons who are:

C2.3.3.1. Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf, of a foreign power;

C2.3.3.2. An organization reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;

C2.3.3.3. Persons or organizations reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities;

C2.3.3.4. Persons who are reasonably believed to be prisoners of war; missing in action; or are the targets, the hostages, or victims of international terrorist organizations; or

C2.3.3.5. Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons.

C2.3.4. <u>Counterintelligence</u>. Information may be collected about a United States person if the information constitutes counterintelligence, provided the intentional collection of counterintelligence about United States persons must be limited to:

C2.3.4.1. Persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.

C2.3.4.2. Persons in contact with persons described in subparagraph C2.3.4.1., above, for the purpose of identifying such person and assessing their relationship with persons described in subparagraph C2.3.4.1., above.

C2.3.5. Potential Sources of Assistance to Intelligence Activities. Information may be collected about United States persons reasonably believed to be potential sources of intelligence, or potential sources of assistance to intelligence activities, for the purpose of assessing their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

C2.3.6. Protection of Intelligence Sources and Methods. Information may be collected about a United States person who has access to, had access to, or is otherwise in possession of, information that reveals foreign intelligence and counterintelligence sources or methods, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information; provided that within the United States, intentional collection of such information shall be limited to persons who are:

C2.3.6.1. Present and former DoD employees;

C2.3.6.2. Present or former employees of a present or former DoD contractor; and

C2.3.6.3. Applicants for employment at the Department of Defense or at a contractor of the Department of Defense.

C2.3.7. Physical Security. Information may be collected about a United States person who is reasonably believed to threaten the physical security of DoD employees, installations, operations, or official visitors. Information may also be collected in the course of a lawful physical security investigation.

C2.3.8. Personnel Security. Information may be collected about a United States person that arises out of a lawful personnel security investigation.

C2.3.9. Communications Security. Information may be collected about a United States person that arises out of a lawful communications security investigation.

C2.3.10. Narcotics. Information may be collected about a United States person who is reasonably believed to be engaged in international narcotics activities.

C2.3.11. Threats to Safety. Information may be collected about a United States person when the information is needed to protect the safety of any person or

organization, including those who are targets, victims, or hostages of international terrorist organizations.

C2.3.12. Overhead Reconnaissance. Information may be collected from overhead reconnaissance not directed at specific United States persons.

C2.3.13. Administrative Purposes. Information may be collected about a United States person that is necessary for administrative purposes.

C2.4. GENERAL CRITERIA GOVERNING THE MEANS USED TO COLLECT INFORMATION ABOUT UNITED STATES PERSONS

C2.4.1. Means of Collection. DoD intelligence components are authorized to collect information about United States persons by any lawful means, provided that all such collection activities shall be carried out in accordance with E.O. 12333 (reference (a)), and this Regulation, as appropriate.

C2.4.2. Least Intrusive Means. The collection of information about United States persons shall be accomplished by the least intrusive means. In general, this means the following:

C2.4.2.1. To the extent feasible, such information shall be collected from publicly available information or with the consent of the person concerned;

C2.4.2.2. If collection from these sources is not feasible or sufficient, such information may be collected from cooperating sources;

C2.4.2.3. If collection from cooperating sources is not feasible or sufficient, such information may be collected, as appropriate, using other lawful investigative techniques that do not require a judicial warrant or the approval of the Attorney General; then

C2.4.2.4. If collection through use of these techniques is not feasible or sufficient, approval for use of investigative techniques that do require a judicial warrant or the approval of the Attorney General may be sought.

C2.5. SPECIAL LIMITATION ON THE COLLECTION OF FOREIGN INTELLIGENCE WITHIN THE UNITED STATES

Within the United States, foreign intelligence concerning United States persons may be collected only by overt means unless all the following conditions are met:

C2.5.1. The foreign intelligence sought is significant and collection is not undertaken for the purpose of acquiring information concerning the domestic activities of any United States person;

C2.5.2. Such foreign intelligence cannot be reasonably obtained by overt means;

C2.5.3. The collection of such foreign intelligence has been coordinated with the Federal Bureau of Investigation (FBI); and

C2.5.4. The use of other than overt means has been approved in writing by the head of the DoD intelligence component concerned, or his single designee, as being consistent with these procedures. A copy of any approval made pursuant to this section shall be provided the Deputy Under Secretary of Defense (Policy).

C3. CHAPTER 3

PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS

C3.1. APPLICABILITY

This procedure governs the kinds of information about United States persons that may knowingly be retained by a DoD intelligence component without the consent of the person whom the information concerns. It does not apply when the information in question is retained solely for administrative purposes or is required by law to be maintained.

C3.2. EXPLANATION OF UNDEFINED TERMS

The term "retention," as used in this procedure, refers only to the maintenance of information about United States persons that can be retrieved by reference to the person's name or other identifying data.

C3.3. CRITERIA FOR RETENTION

C3.3.1. Retention of Information Collected Under Procedure 2. Information about United States persons may be retained if it was collected pursuant to Procedure 2.

C3.3.2. Retention of Information Acquired Incidentally. Information about United States persons collected incidentally to authorized collection may be retained if:

C3.3.2.1. Such information could have been collected intentionally under Procedure 2;

C3.3.2.2. Such information is necessary to understand or assess foreign intelligence or counterintelligence;

C3.3.2.3. The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with this Regulation; or

C3.3.2.4. Such information is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.

C3.3.3. Retention of Information Relating to Functions of Other DoD Components or non-DoD Agencies. Information about United States persons that pertains solely to the functions of other DoD Components or Agencies outside the Department of Defense shall be retained only as necessary to transmit or deliver such information to the appropriate recipients.

C3.3.4. Temporary Retention. Information about United States persons may be retained temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be permanently retained under these procedures.

C3.3.5. Retention of Other Information. Information about United States persons other than that covered by paragraphs C3.3.1. through C3.3.4., above, shall be retained only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

C3.4. ACCESS AND RETENTION

C3.4.1. Controls On Access to Retained Information. Access within a DoD intelligence component to information about United States persons retained pursuant to this procedure shall be limited to those with a need to know.

C3.4.2. Duration of Retention. Disposition of information about United States Persons retained in the files of DoD intelligence components will comply with the disposition schedules approved by the Archivist of the United States for the files or records in which the information is retained.

C3.4.3. Information Acquired Prior to Effective Date. Information acquired prior to the effective date of this procedure may be retained by DoD intelligence components without being screened for compliance with this procedure or Executive Order 12333 (reference (a)), so long as retention was in compliance with applicable law and previous Executive orders.

C4. CHAPTER 4

PROCEDURE 4. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS

C4.1. APPLICABILITY AND SCOPE

This procedure governs the kinds of information about United States persons that may be disseminated, without their consent, outside the DoD intelligence component that collected and retained the information. It does not apply to information collected solely for administrative purposes; or disseminated pursuant to law; or pursuant to a court order that otherwise imposes controls upon such dissemination.

C4.2. CRITERIA FOR DISSEMINATION

Except as provided in section C4.3., below, information about United States persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions:

C4.2.1. The information was collected or retained or both under Procedures 2 and 3;

C4.2.2. The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following:

C4.2.2.1. An employee of the Department of Defense, or an employee of a contractor of the Department of Defense, and has a need for such information in the course of his or her official duties;

C4.2.2.2. A law enforcement entity of Federal, State, or local government, and the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce;

C4.2.2.3. An Agency within the intelligence community; provided that within the intelligence community, information other than information derived from signals intelligence, may be disseminated to each appropriate Agency for the purpose of allowing the recipient Agency to determine whether the information is relevant to its responsibilities without such a determination being required of the disseminating DoD intelligence component;

C4.2.2.4. An Agency of the Federal Government authorized to receive such information in the performance of a lawful governmental function; or

C4.2.2.5. A foreign government, and dissemination is undertaken pursuant to an agreement or other understanding with such government.

C4.3. OTHER DISSEMINATION

Any dissemination that does not conform to the conditions set forth in section C4.2., above, must be approved by the legal office responsible for advising the DoD Component concerned after consultation with the Department of Justice and General Counsel of the Department of Defense. Such approval shall be based on determination that the proposed dissemination complies with applicable laws, Executive orders, and regulations.

C5. CHAPTER 5

PROCEDURE 5. ELECTRONIC SURVEILLANCE

C5.1. PART 1: ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.1.1. Applicability. This part of Procedure 5 implements the Foreign Intelligence Surveillance Act of 1979 (reference (b)), and applies to electronic surveillance, as defined in that Act, conducted by DoD intelligence components within the United States to collect "foreign intelligence information," as defined in that Act.

C5.1.2. General Rules

C5.1.2.1. Electronic Surveillance Pursuant to the Foreign Intelligence Surveillance Act. A DoD intelligence component may conduct electronic surveillance within the United States for foreign intelligence and counterintelligence purposes only pursuant to an order issued by a judge of the court appointed pursuant to the Foreign Intelligence Surveillance Act of 1978 (reference (b)), or pursuant to a certification of the Attorney General issued under the authority of Section 102(a) of the Act.

C5.1.2.2. Authority to Request Electronic Surveillance. Authority to approve the submission of applications or requests for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (reference (b)) shall be limited to the Secretary of Defense, the Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, and the Director of the National Security Agency. Applications for court orders will be made through the Attorney General after prior clearance by the General Counsel, DoD. Requests for Attorney General certification shall be made only after prior clearance by the General Counsel, DoD.

C5.1.2.3. Electronic Surveillance In Emergency Situations

C5.1.2.3.1. A DoD intelligence component may conduct electronic surveillance within the United States in emergency situations under an approval from the Attorney General in accordance with Section 105(e) of reference (b).

C5.1.2.3.2. The head of a DoD intelligence component may request that the DoD General Counsel seek such authority directly from the Attorney General in an emergency, if it is not feasible to submit such request through an official designated in subparagraph C5.1.2.2., above, provided the appropriate official concerned shall be advised of such requests as soon as possible thereafter.

C5.2. PART 2: ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.2.1. Applicability. This part of Procedure 5 applies to electronic surveillance, as defined in the Definitions Section, for foreign intelligence and counterintelligence purposes directed against United States persons who are outside the United States, and who, under the circumstances, have a reasonable expectation of privacy. It is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Part 1 and the regulation of "signals intelligence activities" under Part 3 so that the intentional interception for foreign intelligence and counterintelligence purposes of all wire or radio communications of persons within the United States and against United States persons abroad where such persons enjoy a reasonable expectation of privacy is covered by one of the three parts. In addition, this part governs the use of electronic, mechanical, or other surveillance devices for foreign intelligence and counterintelligence purposes against a United States person abroad in circumstances where such person has a reasonable expectation of privacy. This part does not apply to the electronic surveillance of communications of other than United States persons abroad or the interception of the communications of United States persons abroad that do not constitute electronic surveillance.

C5.2.2. Explanation of Undefined Terms

C5.2.2.1. Electronic surveillance is "directed against a United States person" when the surveillance is intentionally targeted against or designed to intercept the communications of that person. Electronic surveillance directed against persons who are not United States persons that results in the incidental acquisition of the communications of a United States person does not thereby become electronic surveillance directed against a United States person.

C5.2.2.2. Electronic surveillance is "outside the United States" if the person against whom the electronic surveillance is directed is physically outside the United States, regardless of the location at which surveillance is conducted. For example, the interception of communications that originate and terminate outside the United States can be conducted from within the United States and still fall under this part rather than Part 1.

C5.2.3. Procedures. Except as provided in paragraph C5.2.5., below, DoD intelligence components may conduct electronic surveillance against a United States person who is outside the United States for foreign intelligence and counterintelligence purposes only if the surveillance is approved by the Attorney General. Requests for

approval will be forwarded to the Attorney General by an official designated in subparagraph C5.2.5.1., below. Each request shall include:

C5.2.3.1. An identification or description of the target.

C5.2.3.2. A statement of the facts supporting a finding that:

C5.2.3.2.1. There is probable cause to believe the target of the electronic surveillance is one of the following:

C5.2.3.2.1.1. A person who, for or on behalf of a foreign power is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaging in such activities;

C5.2.3.2.1.2. A person who is an officer or employee of a foreign power;

C5.2.3.2.1.3. A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this paragraph, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

C5.2.3.2.1.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

C5.2.3.2.1.5. A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

C5.2.3.2.2. The electronic surveillance is necessary to obtain significant foreign intelligence or counterintelligence.

C5.2.3.2.3. The significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance could not reasonably be obtained by other less intrusive collection techniques.

C5.2.3.3. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance.

C5.2.3.4. A description of the means by which the electronic surveillance will be effected.

C5.2.3.5. If physical trespass is required to effect the surveillance, a statement of facts supporting a finding that the means involve the least amount of intrusion that will accomplish the objective.

C5.2.3.6. A statement of period of time, not to exceed 90 days, for which the electronic surveillance is required.

C5.2.3.7. A description of the expected dissemination of the product of the surveillance, including a description of the procedures that will govern the retention and dissemination of communications of or concerning United States persons other than those targeted, acquired incidental to such surveillance.

C5.2.4. Electronic Surveillance in Emergency Situations. Notwithstanding paragraph C5.2.3., above, a DoD intelligence component may conduct surveillance directed at a United States person who is outside the United States in emergency situations under the following limitations:

C5.2.4.1. Officials designated in paragraph C5.2.5., below, may authorize electronic surveillance directed at a United States person outside the United States in emergency situations, when securing the prior approval of the Attorney General is not practical because:

C5.2.4.1.1. The time required would cause failure or delay in obtaining significant foreign intelligence or counterintelligence and such failure or delay would result in substantial harm to the national security;

C5.2.4.1.2. A person's life or physical safety is reasonably believed to be in immediate danger; or

C5.2.4.1.3. The physical security of a defense installation or Government property is reasonably believed to be in immediate danger.

C5.2.4.2. Except for actions taken under subparagraph C5.2.4.1.2., above, any official authorizing such emergency surveillance shall find that one of the criteria contained in subparagraph C5.2.3.2.1., above, is met. Such officials shall notify the DoD General Counsel promptly of any such surveillance, the reason for authorizing such surveillance on an emergency basis, and the expected results.

C5.2.4.3. The Attorney General shall be notified by the General Counsel, DoD, as soon as possible of the surveillance, the circumstances surrounding its authorization, and the results thereof, and such other information as may be required to authorize continuation of such surveillance.

C5.2.4.4. Electronic surveillance authorized pursuant to this section may not continue longer than the time required for a decision by the Attorney General and in no event longer than 72 hours.

C5.2.5. Officials Authorized to Request and Approve Electronic Surveillance Outside the United States

C5.2.5.1. The following officials may request approval of electronic surveillance outside the United States under paragraph C5.2.3., above, and approve emergency surveillance under paragraph C5.2.4., above:

C5.2.5.1.1. The Secretary and Deputy Secretary of Defense.

C5.2.5.1.2. The Secretaries and Under Secretaries of the Military Departments.

C5.2.5.1.3. The Director and Deputy Director of the National Security Agency/Chief, Central Security Service.

C5.2.5.2. Authorization for emergency electronic surveillance under paragraph C5.2.4., may also be granted by:

C5.2.5.2.1. Any general or flag officer at the overseas location in question, having responsibility for either the subject of the surveillance, or responsibility for the protection of the persons, installations, or property that is endangered, or

C5.2.5.2.2. The Deputy Director for Operations, National Security Agency.

C5.3. PART 3: SIGNALS INTELLIGENCE ACTIVITIES

C5.3.1. Applicability and Scope

C5.3.1.1. This procedure governs the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection,

retention, and dissemination of foreign communications and military tactical communications. Such activities may incidentally involve the collection of information concerning United States persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of a party thereto.

C5.3.1.2. This part of Procedure 5 shall be supplemented by a classified Annex promulgated by the Director, National Security Agency/Chief, Central Security Service, which shall also be approved by the Attorney General. That regulation shall provide that signals intelligence activities that constitute electronic surveillance, as defined in Parts 1, and 2 of this procedure, will be authorized in accordance with those parts. Any information collected incidentally about United States persons shall be subjected to minimization procedures approved by the Attorney General.

C5.3.2. Explanation of Undefined Terms

C5.3.2.1. Communications concerning a United States person are those in which the United States person is identified in the communication. A United States person is identified when the person's name, unique title, address or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A reference to a product by brand name or manufacturer's name or the use of a name in a descriptive sense, as, for example, "Monroe Doctrine," is not an identification of a United States person.

C5.3.2.2. Interception means the acquisition by the United States Signals Intelligence system through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signals.

C5.3.2.3. Military tactical communications means United States and allied military exercise communications within the United States and abroad necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

C5.3.2.4. United States Person. For purposes of signals intelligence activities only, the following guidelines will apply in determining whether a person is a United States person:

C5.3.2.4.1. A person known to be currently in the United States will be treated as a United States person unless the nature of the person's communications or other available information concerning the person gives rise to a reasonable belief that such person is not a United States citizen or permanent resident alien.

C5.3.2.4.2. A person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien.

C5.3.2.4.3. A person known to be an alien admitted for permanent residence may be assumed to have lost status as a United States person if the person leaves the United States and it is known that the person is not in compliance with the administrative formalities provided by law that enable such persons to reenter the United States without regard to the provisions of law that would otherwise restrict an alien's entry into the United States. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

C5.3.2.4.4. An unincorporated association whose headquarters are located outside the United States may be presumed not to be a United States person unless the collecting agency has information indicating that a substantial number of members are citizens of the United States or aliens lawfully admitted for permanent residence.

C5.3.2.5. <u>United States Signals Intelligence System</u> means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the Military Services authorized to conduct signals intelligence and such other entities (other than the Federal Bureau of Investigation) as are authorized by the National Security Council or the Secretary of Defense to conduct signals intelligence. FBI activities are governed by procedures promulgated by the Attorney General.

C5.3.3. <u>Procedures</u>

C5.3.3.1. <u>Foreign Communications</u>. The United States Signals Intelligence System may collect, process, retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this procedure.

C5.3.3.2. Military Tactical Communications. The United States Signals Intelligence System may collect, process, retain, and disseminate military tactical communications that are also communications of or concerning United States persons but only in accordance with the classified annex to this procedure.

C5.3.3.2.1. Collection. Collection efforts will be conducted in the same manner as in the case of signals intelligence for foreign intelligence purposes and must be designed in such a manner as to avoid to the extent feasible the intercept of communications not related to military exercises.

C5.3.3.2.2. Retention and Processing. Military tactical communications may be retained and processed without deletion of references to United States persons who are participants in, or are otherwise mentioned in exercise-related communications, provided that the communications of United States persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible.

C5.3.3.2.3. Dissemination. Dissemination of military tactical communications and exercise reports or information files derived from such communications shall be limited to those authorities and persons participating in or conducting reviews and critiques of such exercise.

C5.4. PART 4: TECHNICAL SURVEILLANCE COUNTERMEASURES

C5.4.1. Applicability and Scope. This part of Procedure 5 applies to the use of electronic equipment to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance. It implements Section 105(f)(2) of the Foreign Intelligence Surveillance Act (reference (b)).

C5.4.2. Explanation of Undefined Terms. The term technical surveillance countermeasures refers to activities authorized pursuant to DoD Directive 5200.29 (reference (c)), and, as used in this procedure, refers to the use of electronic surveillance equipment, or electronic or mechanical devices, solely for determining the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, or for determining the susceptibility of electronic equipment to unlawful electronic surveillance.

C5.4.3. Procedures A DoD intelligence component may use technical surveillance countermeasures that involve the incidental acquisition of the nonpublic communications of United States persons without their consent, provided:

C5.4.3.1. The use of such countermeasures has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken;

C5.4.3.2. The use of such countermeasures is limited in that necessary to determine the existence and capability of such equipment; and

C5.4.3.3. Access to the content of communications acquired during the use of countermeasures is limited to persons involved directly in conducting such measures, and any content acquired is destroyed as soon as practical or upon completion of the particular use. However, if the content is acquired within the United States, only information that is necessary to protect against unauthorized electronic surveillance, or to enforce Chapter 119 of title 18, United States Code (reference (d)) and Section 605 of the Communication Act of 1934 (reference (e)), may be retained and disseminated only for these purposes. If acquired outside the United States, information that indicates a violation of Federal law, including the Uniform Code of Military Justice (reference (f)), or a clear and imminent threat to life or property, may also be disseminated to appropriate law enforcement authorities. A record of the types of communications and information subject to acquisition by the illegal electronic surveillance equipment may be retained.

C5.5. PART 5: DEVELOPING, TESTING, AND CALIBRATION OF ELECTRONIC EQUIPMENT

C5.5.1. Applicability This part of Procedure 5 applies to developing, testing, or calibrating electronic equipment that can intercept or process communications and non-communications signals. It also includes research and development that needs electronic communications as a signal source.

C5.5.2. Procedures

C5.5.2.1. Signals Authorized for Use

C5.5.2.1.1. The following may be used without restriction:

C5.5.2.1.1.1. Laboratory-generated signals.

C5.5.2.1.1.2. Communications signals with the consent of the communicator.

C5.5.2.1.1.3. Communications in the commercial or public service broadcast bands.

C5.5.2.1.1.4. Communications transmitted between terminals located outside of the United States not used by any known United States person.

C5.5.2.1.1.5. Non-communications signals (including telemetry, and radar).

C5.5.2.1.2. Communications subject to lawful electronic surveillance under the provisions of Parts 1, 2, or 3, of this procedure may be used subject to the minimization procedures applicable to such surveillance.

C5.5.2.1.3. Any of the following may be used subject to the restrictions of subparagraph C5.5.2.2., below.

C5.5.2.1.3.1. Communications over official Government communications circuits with consent from an appropriate official of the controlling agency.

C5.5.2.1.3.2. Communications in the citizens and amateur-radio bands.

C5.5.2.1.4. Other signals may be used only when it is determined that it is not practical to use the signals described above and it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance. The restrictions of subparagraph C5.5.2.2., below, will apply in such cases. The Attorney General must approve use of signals pursuant to this subsection for the purpose of development, testing, or calibration when the period of use exceeds 90 days. When Attorney General approval is required, the DoD intelligence component shall submit a test proposal to the General Counsel, DoD, or the NSA General Counsel for transmission to the Attorney General for approval. The test proposal shall state the requirement for a period beyond 90 days, the nature of the activity, the organization that will conduct the activity, and the proposed disposition of any signals or communications acquired during the activity.

C5.5.2.2. <u>Restrictions</u>. For signals described in subparagraphs C5.5.2.1.3. and C5.5.2.1.4., above, the following restrictions apply:

C5.5.2.2.1. The surveillance shall be limited in scope and duration to that necessary for the purposes referred to in paragraph C5.5.1., above.

C5.5.2.2.2. No particular United States person shall be targeted intentionally without consent.

C5.5.2.2.3. The content of any communication shall:

C5.5.2.2.3.1. Be retained only when actually needed for the purposes referred to in paragraph C5.5.1., above;

C5.5.2.2.3.2. Be disseminated only to persons conducting the activity; and

C5.5.2.2.3.3. Be destroyed immediately upon completion of the activity.

C5.5.2.2.4. The technical parameters of a communication (such as frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purposes outlined in paragraph C5.5.1., above, or for collection avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance or related development, testing, and calibration of electronic equipment provided such dissemination and use are limited to the purposes outlined in paragraph C5.5.1., or collection avoidance purposes. No content of any communication may be retained or used other than as provided in subparagraph C5.5.2.2.3., above.

C5.6. PART 6: TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT

C5.6.1. Applicability. This part of Procedure 5 applies to the training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment. It does not apply to the interception of communications with the consent of one of the parties to the communication or to the training of intelligence personnel by non-intelligence components.

C5.6.2. Procedures

C5.6.2.1. Training Guidance. The training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance

equipment shall include guidance concerning the requirements and restrictions of the Foreign Intelligence Surveillance Act of 1978 (reference (b)), and E.O. 12333 (reference (a)), with respect to the unauthorized acquisition and use of the content of communications of United States persons.

C5.6.2.2. Training Limitations

C5.6.2.2.1. Except as permitted by paragraph C5.6.2.2.2. and C5.6.2.2.3., below, the use of electronic communications and surveillance equipment for training purposes is permitted, subject to the following limitations:

C5.6.2.2.1.1. To the maximum extent practical, use of such equipment for training purposes shall be directed against communications that are subject to lawful electronic surveillance for foreign intelligence and counterintelligence purposes under Parts 1, 2, and 3 of this procedure.

C5.6.2.2.1.2. The contents of private communications of non-consenting United States persons may not be acquired aurally unless the person is an authorized target of electronic surveillance.

C5.6.2.2.1.3. The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

C5.6.2.2.2. Public broadcasts, distress signals, or official U.S. Government communications may be monitored, provided that when Government Agency communications are monitored, the consent of an appropriate official is obtained.

C5.6.2.2.3. Minimal acquisition of information is permitted as required for calibration purposes.

C5.6.2.3. Retention and Dissemination. Information collected during training that involves communications described in subparagraph C5.6.2.2.1.1., above, shall be retained and disseminated in accordance with minimization procedures applicable to that electronic surveillance. Information collected during training that does not involve communications described in subparagraph C5.6.2.2.1.1., above, or that is acquired inadvertently, shall be destroyed as soon as practical or upon completion of the training and may not be disseminated for any purpose. This limitation does not apply to distress signals.

C5.7. PART 7: CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYS

C5.7.1. Applicability and Scope This part of Procedure 5 applies to the conduct of vulnerability surveys and hearability surveys by DoD intelligence components.

C5.7.2. Explanation of Undefined Terms

C5.7.2.1. The term vulnerability survey refers to the acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by foreign intelligence services.

C5.7.2.2. The term hearability survey refers to monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the hearability of reception over time.

C5.7.3. Procedures

C5.7.3.1. Conduct of Vulnerability Surveys. Nonconsensual surveys may be conducted to determine the potential vulnerability to intelligence services of a foreign power of transmission facilities of communications common carriers, other private commercial entities, and entities of the federal government, subject of the following limitations:

C5.7.3.1.1. No vulnerability survey may be conducted without the prior written approval of the Director, National Security Agency, or his designee.

C5.7.3.1.2. No transmission may be acquired aurally.

C5.7.3.1.3. No content of any transmission may be acquired by any means.

C5.7.3.1.4. No transmissions may be recorded.

C5.7.3.1.5. No report or log may identify any United States person or entity except to the extent of identifying transmission facilities that are vulnerable to surveillance by foreign powers. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, the identity of such users may be obtained but not from the content of the transmissions themselves, and may be included in such report or log. Reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.

C5.7.3.2. Conduct of Hearability Surveys. The Director, National Security Agency, may conduct, or may authorize the conduct by other Agencies, of hearability surveys of telecommunications that are transmitted in the United States.

C5.7.3.2.1. Collection. When practicable, consent will be secured from the owner or user of the facility against which the hearability survey is to be conducted prior to the commencement of the survey.

C5.7.3.2.2. Processing and Storage. Information collected during a hearability survey must processed and stored as follows:

C5.7.3.2.2.1. The content of communications may not be recorded or included in any report.

C5.7.3.2.2.2. No microwave transmission may be de-multiplexed or demodulated for any purpose.

C5.7.3.2.2.3. No report or log may identify any person or entity except to the extent of identifying the transmission facility that can be intercepted from the intercept site. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, and their identities are relevant to the purpose for which the hearability survey has been conducted, the identity of such users may be obtained provided such identities may not be obtained from the contents of the transmissions themselves.

C5.7.3.2.3. Dissemination. Reports may be disseminated only within the U.S. Government. Logs may not be disseminated unless required to verify results contained in reports.

C6. CHAPTER 6

PROCEDURE 6. CONCEALED MONITORING

C6.1. APPLICABILITY AND SCOPE

C6.1.1. This procedure applies to concealed monitoring only for foreign intelligence and counterintelligence purposes conducted by a DoD intelligence component within the United States or directed against a United States person who is outside the United States where the subject of such monitoring does not have a reasonable expectation of privacy, as explained in section 6.2., below, and no warrant would be required if undertaken for law enforcement purposes.

C6.1.2. Concealed monitoring in the United States for foreign intelligence and counterintelligence purposes where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance within the United States" under Part 1 of Procedure 5, and processed pursuant to that procedure.

C6.1.3. Concealed monitoring for foreign intelligence and counterintelligence purposes of a United States person abroad where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance outside the United States" under Part 2 of Procedure 5, and processed pursuant to that procedure.

C6.1.4. Concealed monitoring for foreign intelligence and counterintelligence purposes when the monitoring is a signals intelligence activity shall be conducted pursuant to Part 3 of Procedure 5.

C6.2. EXPLANATION OF UNDEFINED TERMS

C6.2.1. <u>Concealed monitoring</u> means targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time.

C6.2.2. Monitoring is <u>within the United States</u> if the monitoring device, or the target of the monitoring, is located within the United States.

C6.2.3. Whether concealed monitoring is to occur where the subject has a reasonable expectation of privacy is a determination that depends upon the circumstances of a particular case, and shall be made only after consultation with the legal office responsible for advising the DoD intelligence component concerned. Reasonable expectation of privacy is the extent to which a reasonable person in the particular circumstances involved is entitled to believe his or her actions are not subject to monitoring by electronic, optical, or mechanical devices. For example, there are ordinarily reasonable expectations of privacy in work spaces if a person's actions and papers are not subject to ready observation by others under normal working conditions. Conversely, a person walking out of his or her residence into a public street ordinarily would not have a reasonable expectation that he or she is not being observed or even photographed; however, such a person ordinarily would have an expectation of privacy within his or her residence.

C6.3. PROCEDURES

C6.3.1. Limitations On Use of Concealed Monitoring. Use of concealed monitoring under circumstances when the subject of such monitoring has no reasonable expectation of privacy is subject to the following limitations:

C6.3.1.1. Within the United States, a DoD intelligence component may conduct concealed monitoring only on an installation or facility owned or leased by the Department of Defense or otherwise in the course of an investigation conducted pursuant to the Agreement Between the Secretary of Defense and the Attorney General (reference (g)).

C6.3.1.2. Outside the United States, such monitoring may be conducted on installations and facilities owned or leased by the Department of Defense. Monitoring outside such facilities shall be conducted after coordination with appropriate host country officials, if such coordination is required by the governing Status of Forces Agreement, and with the Central Intelligence Agency.

C6.3.2. Required Determination. Concealed monitoring conducted under paragraph C6.3.1., requires approval by an official designated in paragraph C6.3.3., below, based on a determination that such monitoring is necessary to the conduct of assigned foreign intelligence or counterintelligence functions, and does not constitute electronic surveillance under Parts 1 or 2 of Procedure 5.

C6.3.3. Officials Authorized to Approve Concealed Monitoring. Officials authorized to approve concealed monitoring under this procedure include the Deputy

Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Director, National Security Agency; the Assistant Chief of Staff for Intelligence, Department of Army; the Director, Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, U.S. Air Force; the Commanding General, Army Intelligence and Security Command; the Director, Naval Investigative Service; and the Commanding Officer, Air Force Office of Special Investigations.

C7. CHAPTER 7

PROCEDURE 7. PHYSICAL SEARCHES

C7.1. APPLICABILITY

This procedure applies to nonconsensual physical searches of any person or property within the United States and to physical searches of the person or property of a United States person outside the United States by DoD intelligence components for foreign intelligence or counterintelligence purposes. DoD intelligence components may provide assistance to the Federal Bureau of Investigation and other law enforcement authorities in accordance with Procedure 12.

C7.2. EXPLANATION OF UNDEFINED TERMS

Physical search means any intrusion upon a person or a person's property or possessions to obtain items of property or information. The term does not include examination of areas that are in plain view and visible to the unaided eye if no physical trespass is undertaken, and does not include examinations of abandoned property left in a public place. The term also does not include any intrusion authorized as necessary to accomplish lawful electronic surveillance conducted pursuant to Parts 1 and 2 of Procedure 5.

C7.3. PROCEDURES

C7.3.1. Nonconsensual Physical Searches Within the United States

C7.3.1.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes. The counterintelligence elements of the Military Departments are authorized to conduct nonconsensual physical searches in the United States for counterintelligence purposes of the person or property of active duty military personnel, when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C7.3.1.2., below.

C7.3.1.2. Other Nonconsensual Physical Searches. Except as permitted by section C7.1., above, DoD intelligence components may not conduct nonconsensual physical searches of persons and property within the United States for foreign intelligence or counterintelligence purposes. DoD intelligence components may, however, request the FBI to conduct such searches. All such requests, shall be in writing; shall contain the information required in subparagraphs C7.3.2.2.1., through C7.3.2.2.6., below; and be approved by an official designated in subparagraph C7.3.2.2.3., below. A copy of each such request shall be furnished the General Counsel, DoD.

C7.3.2. Nonconsensual Physical Searches Outside the United States

C7.3.2.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes. The counterintelligence elements of the Military Departments may conduct nonconsensual physical searches of the person or property of active duty military personnel outside the United States for counterintelligence purposes when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C7.3.2.2.2., below.

C7.3.2.2. Other Nonconsensual Physical Searches. DoD intelligence components may conduct other nonconsensual physical searches for foreign intelligence and counterintelligence purposes of the person or property of United States persons outside the United States only pursuant to the approval of the Attorney General. Requests for such approval will be forwarded by a senior official designated in subparagraph C7.3.2.3., below, to the Attorney General and shall include:

C7.3.2.2.1. An identification of the person or description of the property to be searched.

C7.3.2.2.2. A statement of facts supporting a finding that there is probable cause to believe the subject of the search is:

C7.3.2.2.2.1. A person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, activities in preparation for international terrorist activities, or who conspires with, or knowingly aids and abets a person engaging in such activities;

C7.3.2.2.2.2. A person who is an officer or employee of a foreign power;

C7.3.2.2.2.3. A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power does not justify a nonconsensual physical search without evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

C7.3.2.2.2.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

C7.3.2.2.2.5. A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

C7.3.2.2.3. A statement of facts supporting a finding that the search is necessary to obtain significant foreign intelligence or counterintelligence.

C7.3.2.2.4. A statement of facts supporting a finding that the significant foreign intelligence or counterintelligence expected to be obtained could not be obtained by less intrusive means.

C7.3.2.2.5. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the search.

C7.3.2.2.6. A description of the extent of the search and a statement of facts supporting a finding that the search will involve the least amount of physical intrusion that will accomplish the objective sought.

C7.3.2.2.7. A description of the expected dissemination of the product of the search, including a description of the procedures that will govern the retention and dissemination of information about United States persons acquired incidental to the search.

C7.3.2.3. Requests for approval of nonconsensual physical searches under subparagraph C7.3.2.2., must be made by:

C7.3.2.3.1. The Secretary or the Deputy Secretary of Defense;

C7.3.2.3.2. The Secretary or the Under Secretary of a Military Department;

C7.3.2.3.3. The Director, National Security Agency; or

C7.3.2.3.4. The Director, Defense Intelligence Agency.

C8. CHAPTER 8

PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL

C8.1. APPLICABILITY

This procedure applies to the opening of mail in United States postal channels, and the use of mail covers with respect to such mail, for foreign intelligence and counterintelligence purposes. It also applies to the opening of mail to or from United States persons where such activity is conducted outside the United States and such mail is not in United States postal channels.

C8.2. EXPLANATION OF UNDEFINED TERMS

C8.2.1. Mail Within United States Postal Channels includes:

C8.2.1.1. Mail while in transit within, among, and between the United States, its territories and possessions (including mail of foreign origin that is passed by a foreign postal administration, to the United States Postal Service for forwarding to a foreign postal administration under a postal treaty or convention, and mail temporarily in the hands of the United States Customs Service or the Department of Agriculture), Army-Air Force (APO) and Navy (FPO) post offices, and mail for delivery to the United Nations, NY; and

C8.2.1.2. International mail enroute to an addressee in the United States or its possessions after passage to United States Postal Service from a foreign postal administration or enroute to an addressee abroad before passage to a foreign postal administration. As a rule, mail shall be considered in such postal channels until the moment it is delivered manually in the United States to the specific addressee named on the envelope, or his authorized agent.

C8.2.2. To examine mail means to employ a mail cover with respect to such mail.

C8.2.3. Mail cover means the process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the Postal Service.

C8.3. PROCEDURES

C8.3.1. Searches of Mail Within United States Postal Channels

C8.3.1.1. Applicable postal regulations do not permit DoD intelligence components to detain or open first-class mail within United States postal channels for foreign intelligence and counterintelligence purposes, or to request such action by the U.S. Postal Service.

C8.3.1.2. DoD intelligence components may request appropriate U.S. postal authorities to inspect, or authorize the inspection, of the contents of second-, third-, or fourth-class mail in United States postal channels, for such purposes, in accordance with applicable postal regulations. Such components may also request appropriate U.S. postal authorities to detain, or permit the detention of, mail that may become subject to search under this section, in accordance with applicable postal regulations.

C8.3.2. Searches of Mail Outside United States Postal Channels

C8.3.2.1. DoD intelligence components are authorized to open mail to or from a United States person that is found outside United States postal channels only pursuant to the approval of the Attorney General. Requests for such approval shall be treated as a request for a nonconsensual physical search under subparagraph C7.3.2.2., of Procedure 7.

C8.3.2.2. Heads of DoD intelligence components may authorize the opening of mail outside U.S. postal channels when both the sender and intended recipient are other than United States persons if such searches are otherwise lawful and consistent with any Status of Forces Agreement that may be in effect.

C8.3.3. Mail Covers

C8.3.3.1. DoD intelligence components may request U.S. postal authorities to examine mail in U.S. postal channels, for counterintelligence purposes, in accordance with applicable postal regulations.

C8.3.3.2. DoD intelligence components may also request mail covers with respect to mail to or from a United States person that is outside U.S. postal channels, in accordance with appropriate law and procedure of the host government, and any Status of Forces Agreement that may be effect.

C9. CHAPTER 9

PROCEDURE 9. PHYSICAL SURVEILLANCE

C9.1. APPLICABILITY

This procedure applies only to the physical surveillance of United States persons by DoD intelligence components for foreign intelligence and counterintelligence purposes. This procedure does not apply to physical surveillance conducted as part of a training exercise when the subjects are participants in the exercise.

C9.2. EXPLANATION OF UNDEFINED TERMS

The term physical surveillance means a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance.

C9.3. PROCEDURES

C9.3.1. Criteria for Physical Surveillance In the United States. Within the United States, DoD Intelligence components may conduct nonconsensual physical surveillances for foreign intelligence and counterintelligence purposes against United States persons who are present or former employees of the intelligence component concerned; present or former contractors of such components or their present or former employees; applicants for such employment or contracting; or military persons employed by a non-intelligence element of a Military Service. Any physical surveillance within the United States that occurs outside a DoD installation shall be coordinated with the FBI and other law enforcement agencies, as may be appropriate.

C9.3.2. Criteria for Physical Surveillance Outside the United States. Outside the United States, DoD Intelligence components may conduct nonconsensual physical surveillance of United States persons in one of the categories identified in paragraph C9.3.1., above. In addition, such components may conduct physical surveillance of other United States persons in the course of a lawful foreign intelligence or counterintelligence investigation, provided:

C9.3.2.1. Such surveillance is consistent with the laws and policy of the host government and does not violate any Status of Forces Agreement that may be in effect;

C9.3.2.2. That physical surveillance of a United States person abroad to collect foreign intelligence may be authorized only to obtain significant information that cannot be obtained by other means.

C9.3.3. Required Approvals for Physical Surveillance

C9.3.3.1. Persons Within DoD Investigative Jurisdiction. Physical surveillances within the United States or that involve United States persons within DoD investigative jurisdiction overseas may be approved by the head of the DoD intelligence component concerned or by designated senior officials of such components in accordance with this procedure.

C9.3.3.2. Persons Outside DoD Investigative Jurisdiction. Outside the United States, physical surveillances of United States persons who are not within the investigative jurisdiction of the DoD intelligence component concerned will be forwarded through appropriate channels to the Deputy Under Secretary of Defense (Policy) for approval. Such requests shall indicate coordination with the Central Intelligence Agency.

C10. CHAPTER 10

PROCEDURE 10. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS

C10.1. APPLICABILITY

This procedure applies to participation by employees of DoD intelligence components in any organization within the United States, or any organization outside the United States that constitutes a United States person, when such participation is on behalf of any entity of the intelligence community. These procedures do not apply to participation in organizations for solely personal purposes.

C10.2. EXPLANATION OF UNDEFINED TERMS

C10.2.1. Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization or person.

C10.2.2. The term organization includes corporations and other commercial organizations, academic institutions, clubs, professional societies, associations, and any other group whose existence is formalized in some manner or otherwise functions on a continuing basis.

C10.2.3. An organization within the United States means all organizations physically located within the geographical boundaries of the United States whether or not they constitute a United States persons. Thus, a branch, subsidiary, or office of an organization within the United States, which is physically located outside the United States, is not considered as an organization within the United States.

C10.2.4. Participation refers to any action undertaken within the structure or framework of the organization involved. Such actions include serving as a representative or agent of the organization; acquiring membership; attending meetings not open to the public, including social functions for the organization as a whole; carrying out the work or functions of the organization; and contributing funds to the organization other than in payment for goods or services. Actions taken outside the organizational framework, however, do not constitute participation. Thus, attendance at meetings or social gatherings that involve organization members, but are not functions or activities of the organization itself does not constitute participation.

C10.2.5. Participation is on behalf of an agency within the intelligence community when an employee is tasked or requested to take action within an organization for the benefit of such agency. Such employee may already be a member of the organization or may be asked to join. Actions undertaken for the benefit of an intelligence agency include collecting information, identifying potential sources or contacts, or establishing and maintaining cover. If a cooperating source furnishes information to an intelligence agency that he or she obtained by participation within an organization, but was not given prior direction or tasking by the intelligence agency to collect such information, then such participation was not on behalf of such agency.

C10.2.6. Participation is solely for personal purposes, if undertaken at the initiative and expense of the employee for the employee's benefit.

C10.3. PROCEDURES FOR UNDISCLOSED PARTICIPATION

Except as permitted herein, employees of DoD intelligence components may participate on behalf of such components in organizations within the United States, or in organizations outside the United States that constitute United States persons, only if their affiliation with the intelligence component concerned is disclosed to an appropriate official of the organization in accordance with section C10.4., below. Participation without such disclosure is permitted only if it is consistent with the limitations set forth in paragraph C10.3.1., below, and has been approved in accordance with paragraph C10.3.2., below.

C10.3.1. Limitations On Undisclosed Participation

C10.3.1.1. Lawful Purpose. No undisclosed participation shall be permitted under this procedure unless it is essential to achieving a lawful foreign intelligence or counterintelligence purpose within the assigned mission of the collecting DoD intelligence component.

C10.3.1.2. Limitations On Use of Undisclosed Participation for Foreign Intelligence Purposes Within the United States. Undisclosed participation may not be authorized within the United States for the purpose of collecting foreign intelligence from or about a United States person, nor to collect information necessary to assess United States persons as potential sources of assistance to foreign intelligence activities. This does not preclude the collection of information about such persons, volunteered by cooperating sources participating in organizations to which such persons belong, however, if otherwise permitted by Procedure 2.

C10.3.1.3. Duration of Participation. Authorization to participate under subparagraphs C10.3.2.1., and C10.3.2.2., shall be limited to the period covered by such participation, which shall be no longer than 12 months. Participation that lasts longer than 12 months shall be re-approved by the appropriate official on an annual basis in accordance with this procedure.

C10.3.1.4. Participation for the Purpose of Influencing the Activities of the Organization or Its Members. No participation under this procedure shall be authorized for the purpose of influencing the activities of the organization in question, or its members, unless such participation is undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power. Any DoD intelligence component that desires to undertake participation for such purpose shall forward its request to the Deputy Under Secretary of Defense (Policy) setting forth the relevant facts justifying such participation and explaining the nature of its contemplated activity. Such participation may be approved by the DUSD(P) with the concurrence of the General Counsel, DoD.

C10.3.2. Required Approvals

C10.3.2.1. Undisclosed Participation That May Be Approved Within the DoD Intelligence Component. Undisclosed participation on behalf of a DoD intelligence component may be authorized with such component under the following circumstances:

C10.3.2.1.1. Participation in meetings open to the public. For purposes of this section, a seminar or conference sponsored by a professional organization that is open to persons of a particular profession, whether or not they are members of the organization itself or have received a special invitation, shall be considered a meeting open to the public.

C10.3.2.1.2. Participation in organizations that permit other persons acknowledged to the organization to be employees of the U.S. Government to participate.

C10.3.2.1.3. Participation in educational or professional organizations for the purpose of enhancing the professional skills, knowledge, or capabilities of employees.

CI0.3.2.1.4. Participation in seminars, forums, conferences, exhibitions, trade fairs, workshops, symposiums, and similar types of meetings, sponsored by organizations in which the employee is a member, has been invited to participate, or

when the sponsoring organization does not require disclosure of the participants' employment affiliations, for the purpose of collecting significant foreign intelligence that is generally made available to participants at such meetings, and does not involve the domestic activities of the organization or its members.

C10.3.2.2. Participation That May Be Approved By Senior Intelligence Officials. Undisclosed participation may be authorized by the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Assistant Chief of Staff for Intelligence, Department of Army; the Commanding General, U.S. Army Intelligence and Security Command; the Director of Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, United States Air Force; the Director, Naval Investigative Service; the Commanding Officer, Air Force Office of Special Investigations; or their single designees, for the following purposes:

C10.3.2.2.1. To collect significant foreign intelligence outside the United States, or from or about other than United States persons within the United States, provided no information involving the domestic activities of the organization or its members may be collected.

C10.3.2.2.2. For counterintelligence purposes, at the written request of the Federal Bureau of Investigation.

C10.3.2.2.3. To collect significant counterintelligence about other than United States persons, or about United States persons who are within the investigative jurisdiction of the Department of Defense, provided any such participation that occurs within the United States shall be coordinated with the Federal Bureau of Investigation.

C10.3.2.2.4. To collect information necessary to identify and assess other than United States persons as potential sources of assistance for foreign intelligence and counterintelligence activities.

C10.3.2.2.5. To collect information necessary to identify United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

C10.3.2.2.6. To develop or maintain cover necessary for the security of foreign intelligence or counterintelligence activities.

C10.3.2.2.7. Outside the United States, to assess United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

C10.4. DISCLOSURE REQUIREMENT

C10.4.1. Disclosure of the intelligence affiliation of an employee of a DoD intelligence component shall be made to an executive officer of the organization in question, or to an official in charge of membership, attendance, or the records of the organization concerned.

C10.4.2. Disclosure may be made by the DoD intelligence component involved, an authorized DoD official, or by another component of the Intelligence Community that is otherwise authorized to take such action on behalf of the DoD intelligence component concerned.

C11. CHAPTER 11

PROCEDURE 11. CONTRACTING FOR GOODS AND SERVICES

C11.1. APPLICABILITY

This procedure applies to contracting or other arrangements with United States persons for the procurement of goods and services by DoD intelligence components within the United States. This procedure does not apply to contracting with government entities, or to the enrollment of individual students in academic institutions. The latter situation is governed by Procedure 10.

C11.2. PROCEDURES

C11.2.1. Contracts with Academic Institutions. DoD intelligence components may enter into a contract for goods or services with an academic institution only if prior to the making of the contract, the intelligence component has disclosed to appropriate officials of the academic institution the fact of sponsorship by a DoD intelligence component.

C11.2.2. Contracts with Commercial Organizations, Private Institutions, and Individuals. Contracting by or for a DoD intelligence component with commercial organizations, private institutions, or private individuals within the United States may be done without revealing the sponsorship of the intelligence component if:

C11.2.2.1. The contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, and other items incident to approved activities; or

C11.2.2.2. There is a written determination by the Secretary or the Under Secretary of a Military Department, the Director of the National Security Agency, the Director of the Defense Intelligence Agency, or the Deputy Under Secretary of Defense (Policy) that the sponsorship of a DoD intelligence component must be concealed to protect the activities of the DoD intelligence component concerned.

C11.3. EFFECT OF NONCOMPLIANCE

No contract shall be void or voidable for failure to comply with this procedure.

C12. CHAPTER 12

PROCEDURE 12. PROVISION OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES

C12.1. APPLICABILITY

This procedure applies to the provision of assistance by DoD intelligence components to law enforcement authorities. It incorporates the specific limitations on such assistance contained in E.O. 12333 (reference (a)), together with the general limitations and approval requirements of DoD Directive 5525.5 (reference (i)).

C12.2. PROCEDURES

C12.2.1. Cooperation with Law Enforcement Authorities. Consistent with the limitations contained in DoD Directive 5525.5 (reference (i)), and paragraph C12.2.2., below, DoD intelligence components are authorized to cooperate with law enforcement authorities for the purpose of:

C12.2.1.1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;

C12.2.1.2. Protecting DoD employees, information, property, and facilities; and

C12.2.1.3. Preventing, detecting, or investigating other violations of law.

C12.2.2. Types of Permissible Assistance. DoD intelligence components may provide the following types of assistance to law enforcement authorities:

C12.2.2.1. Incidentally acquired information reasonably believed to indicate a violation of Federal law shall be provided in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a));

C12.2.2.2. Incidentially acquired information reasonably believed to indicate a violation of State, local, or foreign law may be provided in accordance with procedures adopted by the Heads of DoD Components;

C12.2.2.3. Specialized equipment and facilities may be provided to Federal law enforcement authorities, and, when lives are endangered, to State and local law

enforcement authorities, provided such assistance is consistent with, and has been approved by an official authorized pursuant to, Enclosure 3 of DoD Directive 5525.5 (reference (i)); and

C12.2.2.4. Personnel who are employees of DoD intelligence components may be assigned to assist Federal law enforcement authorities, and, when lives are endangered, State and local law enforcement authorities, provided such use is consistent with, and has been approved by an official authorized pursuant to, Enclosure 4 of DoD Directive 5525.5 (reference (i)). Such official shall ensure that the General Counsel of the providing DoD Component concurs in such use.

C12.2.2.5. Assistance may be rendered to law enforcement agencies and security services of foreign governments or international organizations in accordance with established policy and applicable Status of Forces Agreements; provided, that DoD intelligence components may not request or participate in activities of such agencies undertaken against United States persons that would not be permitted such components under these procedures.

C13. CHAPTER 13

PROCEDURE 13. EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES

C13.1. APPLICABILITY

This procedure applies to experimentation on human subjects if such experimentation is conducted by or on behalf of a DoD intelligence component. This procedure does not apply to experimentation on animal subjects.

C13.2. EXPLANATION OF UNDEFINED TERMS

C13.2.1. Experimentation in this context means any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives.

C13.2.2. Experimentation is conducted on behalf of a DoD intelligence component if it is conducted under contract to that component or to another DoD Component for the benefit of the intelligence component or at the request of such a component regardless of the existence of a contractual relationship.

C13.2.3. Human subjects in this context includes any person whether or not such person is a United States person.

C13.3. PROCEDURES

C13.3.1. Experimentation on human subjects conducted by or on behalf of a DoD intelligence component may be undertaken only with the informed consent of the subject, in accordance with guidelines issued by the Department of Health and Human Services, setting out conditions that safeguard the welfare of such subjects.

C13.3.2. DoD intelligence components may not engage in or contract for experimentation on human subjects without approval of the Secretary or Deputy Secretary of Defense, or the Secretary or Under Secretary of a Military Department, as appropriate.

C14. CHAPTER 14

PROCEDURE 14. EMPLOYEE CONDUCT

C14.1. APPLICABILITY

This procedure sets forth the responsibilities of employees of DoD intelligence components to conduct themselves in accordance with this Regulation and other applicable policy. It also provides that DoD intelligence components shall ensure, as appropriate, that these policies and guidelines are made known to their employees.

C14.2. PROCEDURES

C14.2.1. Employee Responsibilities. Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 (reference (a)) and this Regulation. In conducting such activities, employees shall not exceed the authorities granted the employing DoD intelligence component by law; Executive order, including E.O. 12333 (reference (a)), and applicable DoD Directives.

C14.2.2. Familiarity With Restrictions

C14.2.2.1. Each DoD intelligence component shall familiarize its personnel with the provisions of E.O. 12333 (reference (a)), this Regulation, and any instructions implementing this Regulation that apply to the operations and activities of such component. At a minimum, such familiarization shall contain:

C14.2.2.1.1. Applicable portions of Procedures 1 through 4;

C14.2.2.1.2. A summary of other procedures that pertains to collection techniques that are, or may be, employed by the DoD intelligence component concerned; and

C14.2.2.1.3. A statement of individual employee reporting responsibility under Procedure 15.

C14.2.2.2. The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IQ)) and each Inspector General responsible for a DoD intelligence component shall ensure, as part of their inspections, that procedures are in effect that will achieve the objectives set forth in subparagraph C14.2.2.1., above.

C14.2.3. Responsibilities of the Heads of DoD Components. The Heads of DoD Components that constitute, or contain, DoD intelligence components shall:

C14.2.3.1. Ensure that all proposals for intelligence activities that may be unlawful, in whole or in part, or may be contrary to applicable Executive Branch or DoD policy are referred to the General Counsel responsible for such component.

C14.2.3.2. Ensure that no adverse action is taken against any employee because the employee reports activities pursuant to Procedure 15.

C14.2.3.3. Impose such sanctions as may be appropriate upon any employee who violates the provisions of this Regulation or any instruction promulgated thereunder.

C14.2.3.4. In any case involving serious or continuing breaches of security by either DoD or non-DoD employees, recommend to the Secretary of Defense appropriate investigative actions.

C14.2.3.5. Ensure that the General Counsel and Inspector General with responsibility for the component, as well as the General Counsel, DoD, and the ATSD(IO), have access to all information concerning the intelligence activities of that component necessary to perform their oversight responsibilities.

C14.2.3.6. Ensure that employees cooperate fully with the Intelligence Oversight Board and its representatives.

C15. CHAPTER 15

PROCEDURE 15. IDENTIFYING, INVESTIGATING, AND REPORTING QUSTIONABLE ACTIVITIES

C15.1. APPLICABILITY

This procedure provides for the identification, investigation, and reporting of questionable intelligence activities.

C15.2. EXPLANATION OF UNDEFINED TERMS

C15.2.1. The term "questionable activity," as used herein, refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive order or Presidential directive, including E.O. 12333 (reference (a)), or applicable DoD policy, including this Regulation.

C15.2.2. The terms "General Counsel"and "Inspector General," as used herein, refer, unless otherwise specified, to any General Counsel or Inspector General with responsibility for one or more DoD intelligence components. Unless otherwise indicated, the term "Inspector General" shall also include the ATSD(IO).

C15.3. PROCEDURES

C15.3.1. Identification

C15.3.1.1. Each employee shall report any questionable activity to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the General Counsel, DoD, or ATSD(IO).

C15.3.1.2. Inspectors General, as part of their inspection of DoD intelligence components, and General Counsels, as part of their oversight responsibilities shall seek to determine if such components are involved in any questionable activities. If such activities have been or are being undertaken, the matter shall be investigated under paragraph C15.3.2., below. If such activities have been undertaken, but were not reported, the Inspector General shall also ascertain the reason for such failure and recommend appropriate corrective action.

C15.3.1.3. Inspectors General, as part of their oversight responsibilities, shall, as appropriate, ascertain whether any organizations, staffs, or offices within their respective jurisdictions, but not otherwise specifically identified as DoD intelligence components, are being used for foreign intelligence or counterintelligence purposes to which Part 2 of E.O. 12333 (reference (a)), applies, and, if so, shall ensure the activities of such components are in compliance with this Regulation and applicable DoD policy.

C15.3.1.4. Inspectors General, as part of their inspection of DoD intelligence components, shall ensure that procedures exist within such components for the reporting of questionable activities, and that employees of such components are aware of their responsibilities to report such activities.

C15.3.2. Investigation

C15.3.2.1. Each report of a questionable activity shall be investigated to the extent necessary to determine the facts and assess whether the activity is legal and is consistent with applicable policy.

C15.3.2.2. When appropriate, questionable activities reported to a General Counsel shall be referred to the corresponding Inspector General for investigation, and if reported to an Inspector General, shall be referred to the corresponding General Counsel to determine whether the activity is legal and consistent with applicable policy. Reports made to the DoD General Counsel or the ATSD(IO) may be referred, after consultation between these officials, to the appropriate Inspector General and General Counsel for investigation and evaluation.

C15.3.2.3. Investigations shall be conducted expeditiously. The officials responsible for these investigations may, in accordance with established procedures, obtain assistance from within the component concerned, or from other DoD Components, when necessary, to complete such investigations in a timely manner.

C15.3.2.4. To complete such investigations, General Counsels and Inspectors General shall have access to all relevant information regardless of classification or compartmentation.

C15.3.3. Reports

C15.3.3.1. Each General Counsel and Inspector General shall report immediately to the General Counsel, DoD, and the ATSD(IO) questionable activities of a serious nature.

C15.3.3.2. Each General Counsel and Inspector General shall submit to the ATSD(IO) a quarterly report describing those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to Executive order or Presidential directive, or applicable DoD policy; and actions taken with respect to such activities. The reports shall also include significant oversight activities undertaken during the quarter and any suggestions for improvements in the oversight system. Separate, joint, or consolidated reports may be submitted. These reports should be prepared in accordance with DoD Directive 5000.11 (reference (j)).

C15.3.3.3. All reports made pursuant to subparagraphs C15.3.3.1., and C15.3.3.2., above, which involve a possible violation of Federal criminal law shall be considered by the General Counsel concerned in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a)).

C15.3.3.4. The General Counsel, DoD, and the ATSD(IO) may review the findings of other General Counsels and Inspectors General with respect to questionable activities.

C15.3.3.5. The ATSD(IO) and the General Counsel, DoD, shall report in a timely manner to the White House Intelligence Oversight Board all activities that come to their attention that are reasonably believed to be illegal or contrary to Executive order or Presidential directive. They will also advise appropriate officials of the Office of the Secretary of Defense of such activities.

C15.3.3.6. These reporting requirements are exempt from format approval and licensing in accordance with paragraph VII.G. of Enclosure 3 to DoD Directive 5000.19 (reference (k)).

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 1-23

Issue Date: 11 March 2004
Revised: 27 December 2007,
29 May 2009

(U) PROCEDURES GOVERNING NSA/CSS ACTIVITIES THAT AFFECT U.S. PERSONS

(U) PURPOSE AND SCOPE

(U) This Policy is issued to comply with DoD Directive 5240.01 (Reference a), which implements 50 U.S.C. 1801 et seq (the Foreign Intelligence Surveillance Act of 1978, as amended (Reference b)); Executive Order 12333, as amended (Reference c); and Executive Order 12863 (Reference d). It establishes procedures and assigns responsibilities to ensure that the signals intelligence and information assurance missions of NSA/CSS are conducted in a manner consistent with the privacy rights of *U.S. persons* and as required by law, executive orders, Department of Defense policies and instructions, and internal NSA/CSS policy.

(U) This Policy applies to all NSA/CSS elements.

//s//

MICHAEL V. HAYDEN
Lieutenant General, USAF
Director, NSA/Chief, CSS

Endorsed by
Associate Director for Policy

Encl:
(U) Annex – Classified Annex to DoD Procedures under Executive Order 12333

DISTRIBUTION:
DJP1
DJP2 (VR)
DJP2 (Archives)

Derived From: NSA/CSSM 1-52
Dated: 20070108
~~Declassify On: 20291123~~

(U) This Policy 1-23 supersedes Directive 10-30, dated 20 September 1990, and Change One thereto, dated June 1998. The Associate Director for Policy endorsed an administrative update, effective 27 December 2007 to make minor adjustments to the policy. This 29 May 2009 administrative update includes changes due to the FISA Amendments Act of 2008 and in core training requirements.
(U) OPI: Office of General Counsel (OGC), 963-3121s
(U) No section of this document, regardless of classification, shall be released without approval from the Office of Policy and Records, DJP1.

(U) POLICY

1. (U) NSA/CSS shall collect, process, retain, and disseminate information about U.S. persons only as prescribed in DoD Directive 5240.1 (Reference a), DoD Regulation 5240.1-R (Reference e), orders issued by the Foreign intelligence Surveillance Court pursuant to reference b, and the Classified Annex to DoD Procedures under Executive Order 12333 (hereafter referred to as the Classified Annex; Reference f).

(U) PROCEDURES

2. (U) Signals Intelligence. The signals intelligence (*SIGINT*) mission of the NSA/CSS is to collect, process, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions. NSA/CSS shall intentionally collect only foreign communications. NSA/CSS shall not intentionally collect U.S. person communications without proper legal authorization. The Director, NSA/Chief, CSS (DIRNSA/CHCSS) may authorize exceptions only pursuant to the procedures contained in DoD Regulation 5240.1-R (Reference e) and the Classified Annex thereto (Reference f).

a. (U) Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, as amended (Reference b), requires a court order issued by a judge appointed pursuant to the Act or a certification of the Attorney General of the United States and the Director of National Intelligence issued pursuant to Section 105(b) of the Act. The DIRNSA/CHCSS or Deputy Director, NSA (D/DIR) must approve applications for a court order, which must be submitted through the DoD General Counsel to the Attorney General. The DIRNSA/CHCSS or D/DIR may contact the Attorney General in an emergency and the Attorney General may approve the surveillance pending subsequent court proceedings.

b. (U) Electronic surveillance, as defined in Appendix A to DoD Regulation 5240.1-R (Reference e), directed against U.S. persons who are outside the U.S. requires an order by the Foreign Intelligence Surveillance Act Court. In emergency situations (e.g., U.S. hostages overseas), as described in Procedure 5, Part 2., of Reference e, the DIRNSA/CHCSS, D/DIR or Senior Operations Officer at the National Security Operations Center may authorize electronic surveillance, after consulting with the Office

of General Counsel (OGC). The Attorney General shall be notified promptly of any such surveillance.

3. (U) Information Assurance. National Security Directive (NSD) 42 (Reference g) and Executive Order 12333 (Reference c) designated DIRNSA as the National Manager for National Security Systems (e.g. NSA's Information Assurance (IA) mission) as that term is defined by 44 U.S. C. 3542(b)(2) (Reference h). In that capacity, and pursuant to those authorities as well as other applicable laws and policies, DIRNSA's responsibilities include examining national security systems and evaluating their vulnerability to foreign interception and exploitation. NSA, as an element of the Intelligence Community and pursuant to section 2.6(c) of Executive Order 12333, as amended, may provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any U.S. Government department or agency having a national security system or a non-national security system. The Executive Order directs that provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department. The Federal Information Security Management Act of 2002 (Reference i) and implementing procedures agreed to by NSA/CSS and the National Institute of Standards and Technology also authorizes NSA/CSS to provide IA support for US government non-national security systems.

a. (U) Any IA activities undertaken by NSA/CSS, including those involving monitoring of official communications, shall be conducted in strict compliance with law, Executive Order and implementing procedures, and applicable Presidential directive. Any monitoring undertaken for communications security purposes ("COMSEC monitoring") shall be conducted in accordance with the provisions of National Telecommunications and Information Systems Security Directive (NTISSD) No. 600 (Reference j) or other special procedures approved by the Attorney General.

b. (U) In addition to the responsibility to conduct COMSEC monitoring and to examine national security systems for vulnerabilities to foreign exploitation, NSD 42 (Reference g) also requires NSA/CSS to disseminate information on threats to national security systems, regardless of the source of the threat. Title II of the Homeland Security Act of 2002 (Reference k) imposes similar requirements with respect to the protection of the United States' critical infrastructure.

c. (U) Pursuant to NSA/CSS Policy 1-2, "(U) Mission and Functions Statements with Service Level Agreements," (Reference l) and IAD's Mission and Functions Statement (Reference m), IAD performs all functions on behalf of the DIRNSA in fulfilling his role as National Manager for National Security Systems. Accordingly, the Information Assurance Director acts for DIRNSA/CHCSS in the issuance of written approval to conduct the information assurance activities assigned to NSA/CSS, including the conduct of activities that may result in the collection of U.S. person information as defined in DoD Regulation 5240.l-R (Reference e) and other applicable guidance.

(U) RESPONSIBILITIES

4. (U) The NSA General Counsel (GC) and Inspector General (IG) shall:

a. (U) Conduct appropriate oversight to identify and prevent violations of Executive Order (E.O.) 12333, DoD Directive 5240.1 (References c and a), this Policy, and any laws, orders, directives and regulations; and

b. (U) Forward to the Intelligence Oversight Board (IOB) of the President's Intelligence Advisory Board (PIAB), through the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)), reports of activities that they have reason to believe may be unlawful or contrary to Executive Order or Presidential Directive, and other questionable intelligence activities or significant or highly sensitive matters, as well as provide other reports or information that the IOB or ATSD(IO) requires.

5. (U) The NSA Inspector General shall:

a. (U) Conduct regular inspections of NSA/CSS activities for compliance with the law, executive orders, and related directives;

b. ~~(S//REL)~~ Perform general oversight of the SIGINT activities of the [redacted] for compliance with E.O. 12333 (Reference c) and related laws and directives;

c. (U) Establish reporting procedures to be followed by the Directors, Associate Directors and Principal Directors, Chiefs of NSA/CSS Field Activities, and NSA/CSS Representatives regarding their activities and practices;

d. (U) Consult with the NSA General Counsel on matters involving interpretation or possible violations of law, executive orders, or directives;

e. (U) Submit, semiannually, a comprehensive report to the DIRNSA/CHCSS and D/DIR on the results of the IG's oversight activities; and

f. (U) Report, as required by E.O. 12333, E.O. 12863 (References c and d) and other authorities, to the ATSD(IO) and the IOB.

6. (U) The NSA General Counsel shall:

a. (U) Provide legal advice and assistance to all NSA/CSS elements regarding the activities covered by this Policy;

b. (U) Assist NSA/CSS activities as requested in developing such guidelines and working aids as are necessary to ensure compliance with this Policy;

c. (U) Assist the NSA Inspector General in inspections and oversight of NSA/CSS activities, as required;

d. (U) Review and assess for legal implications, as requested by any NSA organization, all new major requirements and internally generated NSA/CSS activities;

e. (U) Advise appropriate NSA organizations of new legislation and case law which may have an impact on NSA/CSS missions, functions, operations, activities, or practices;

f. (U) Prepare and forward through DoD to the Attorney General any proposed changes to existing procedures or new procedures required by E.O. 12333 (Reference c) or FISA, as amended (Reference b);

g. (U) In conjunction with the OIG, report as required by E.O. 12333 and E.O. 12863 (References c and d) to the ATSD(IO) and the PIOB, and provide copies of such reports to DIRNSA/CHCSS and affected NSA/CSS elements;

h. (U) Prepare and process applications for authority to conduct electronic surveillance pursuant to law, Executive Order and policy; and

i. (U) Process requests from any DoD intelligence component, including NSA/CSS, for authority to use signals as described in Procedure 5, Part 5, of DoD Regulation 5240.1-R (Reference e), for periods in excess of 90 days in the development, test, or calibration of electronic equipment that can intercept communications and other electronic surveillance equipment. Forward processed requests to the Attorney General for approval when required.

7. (U) The Directors, Associate Directors, the NSA/CSS Chief of Staff, and Extended Enterprise Commanders/Chiefs shall:

a. (U) Appoint an intelligence oversight coordinator or senior level official to oversee intelligence oversight within each major element;

b. (U) Provide training to all *employees* (including contractors and integrees), except *contractor personnel excluded from core training requirements*, in order to maintain a high degree of sensitivity to, and understanding of, the laws and authorities referenced in this Policy. Such training shall include both core and advanced intelligence oversight training and refresher training with appropriate testing. All employees, except contractor personnel excluded from core training requirements, shall receive core training, and those with exposure to U.S. person information shall receive appropriate advanced training. Training shall be required at least annually (or more often commensurate with the level of exposure to U.S. person information by the employee). Newly hired employees and reassignees, including contractor personnel not excluded from core training requirements and integrees, must be trained upon assignment.

Managers shall keep records of training for all employees. The training must cover: E.O. 12333 (Reference c); Procedures 1-4, 14 and 15 of DoD Regulation 5240.1-R (Reference e); other Procedures of the Regulation that apply to the assigned mission; and this Policy. Employees involved in the SIGINT process must be familiar with U.S. Signals Intelligence Directive SP0018 (USSID SP0018) (Reference n), and employees involved in COMSEC monitoring must be familiar with NTISSD 600 (Reference j).

c. (U) Apply the provisions of this Policy to all activities under their cognizance and ensure that all publications (U.S. Signals Intelligence Directives, National COMSEC Instructions, NSA/CSS Management and Administrative Publications, etc.) and instructions for which they are responsible are in compliance with this Policy;

d. (U) Conduct a periodic review of the activities and practices conducted in or under the cognizance of their respective organizations to ensure consistency with the laws and authorities listed in the References section of this Policy;

e. (U) Ensure that all new major requirements levied on NSA/CSS and the U.S. Cryptologic System or internally generated NSA/CSS activities are considered for review and approval by the General Counsel. All activities that may raise a question of law or regulation must be reviewed by the General Counsel prior to acceptance or execution;

f. (U) Ensure that necessary special security clearances and access authorizations are provided to the General Counsel and Inspector General to enable them to meet their assigned responsibilities;

g. (U) Report as required and otherwise assist the Inspector General and General Counsel in carrying out their responsibilities, to include providing input to the Inspector General for preparing the joint Inspector General/General Counsel/Director, NSA/ CSS quarterly report to the Assistant to the Secretary of Defense (Intelligence Oversight) and the IOB; and

h. (U) Develop, in coordination with the General Counsel and Inspector General as required, such specific guidelines and working aids as are necessary to ensure compliance with this Policy. These guidelines and working aids should be available to employees at all times and must be reviewed by management with employees at least annually.

(U) REFERENCES

8. (U) References:

a. (U) DoD Directive 5240.01, "DoD Intelligence Activities," dated August 27, 2007.

b. (U) "Foreign Intelligence Surveillance Act of 1978," as amended, 50 U.S.C. 1801 et seq.

c. (U) Executive Order 12333, "United States Intelligence Activities," as amended.

d. (U) Executive Order 12863, "President's Foreign Intelligence Advisory Board," dated 13 September 1993.

e. (U) DoD Regulation 5240. l-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," dated 7 December 1982.

f. (U) Classified Annex to Department of Defense Procedures Under Executive Order 12333.

g. (U) National Security Directive (NSD) 42, "National Policy for the Security of National Security Telecommunications and Information Systems," dated 5 July 1990.

h. (U) "Information Technology Reform Act of 1996," Division E of Public Law 104-106, as codified at 40 U.S.C. 1401 et seq. [Intelink]

i. (U) "Federal Information Security Management Act of 2002," Public Law 107–347, date 17 December 2002.

j. (U) National Telecommunications and Information Systems Security Directive No. 600, "Communications Security (COMSEC) Monitoring," dated 10 April 1990.

k. (U) "Homeland Security Act of 2002, Title II ," Public Law 107-296.

l. (U) NSA/CSS Policy 1-2, "(U) Mission and Functions Statements with Service Level Agreements," dated 12 May 2003.

m. (U) NSA/CSS Mission and Functions Statement for Information Assurance Directorate, dated 23 April 2003.

n. (U) United States Signals Intelligence Directive (USSID) SP0018, "Legal Compliance and Minimization Procedures," dated 27 July 1993.

o. (U/~~FOUO~~) Memorandum from the Assistant to the Secretary of Defense to the Director, National Security Agency, "Exemption from Specified Training Requirements Required by Department of Defense (DoD) Regulation 5240.1-R," dated 3 December 2008.

p. (U) National Security Council Intelligence Directive (NSCID) No. 6, "Signals Intelligence," dated 17 February 1972.

(U) DEFINITIONS

9. (U~~//FOUO)~~ Contractor Personnel Excluded from Core Training Requirements – Refer to the Secret//Not Releasable to Foreign Nationals memorandum from the Assistant to the Secretary of Defense, dated 3 December 2008 (Reference o), for contractor personnel in this category.

10. (U) Employee – A person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency. DoD Regulation 5240.1-R (Reference e), Appendix A, Definitions.

11. (U) SIGINT – SIGINT comprises communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, either individually or in combination. Communications intelligence (COMINT) is defined as "technical and intelligence information derived from foreign communications by other than the intended recipients . . ." and " . . . the collection and processing of foreign communications passed by radio, wire, or other electromagnetic means." NSCID 6 (Reference p), Sec. 4(b). Electronics intelligence (ELINT) consists of foreign electromagnetic radiations such as emissions from a radar system. Foreign instrumentation signals intelligence (FISINT) includes signals from telemetry, beaconry, etc.

12. ~~(C//REL)~~ U.S. Person –

a. (U) A citizen of the United States;

b. (U) An alien lawfully admitted for permanent residence in the United States;

c. (U) Unincorporated groups and associations a substantial number of the members of which constitute a or b above, or

d. (U) Corporations incorporated in the United States, including U.S. flag non-governmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them. USSID SP0018 (Reference n), Section 9.18.

(U) ANNEX

(U) CLASSIFIED ANNEX TO DEPARTMENT OF DEFENSE PROCEDURES UNDER EXECUTIVE ORDER 12333

Sec. 1: Applicability and Scope (U)

~~(S//SI)~~ These procedures implement sections 2.3, 2.4, and 2.6 (c) of Executive Order 12333 and supplement Procedure 5 of DoD Regulation 5240.1-R, previously approved by the Secretary of Defense and the Attorney General. They govern the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection, retention and dissemination of communications originated or intended for receipt in the United States, and signals intelligence activities that are directed intentionally against the communications of a United States person who is outside the United States. These procedures also govern the collection, retention and dissemination of information concerning United States persons that is collected by the United States Signals Intelligence System including such activities undertaken by the [redacted] These procedures do not apply to signals intelligence activities that are not required under Executive Order 12333 to be conducted pursuant to procedures approved by the Attorney General. Further, these procedures do not apply to signals intelligence activities directed against the radio communications of air and sea vessels for the purpose of collecting foreign intelligence regarding international narcotics trafficking or in support of federal law enforcement efforts to interdict such trafficking. Such signals intelligence activities are subject to a separate classified annex approved earlier by the Attorney General (See Annex J to United States Signals Intelligence Directive 18). Except for matters expressly authorized herein, the limitations contained in Department of Defense Regulation 5240.1-R also apply to the United States Signals Intelligence System. Reference should be made to those procedures with respect to matters of applicability and scope, definitions, policy and operational procedures not covered herein.

Sec. 2: Definitions (U)

(U) The following additional definitions or supplements to definitions in DoD Regulation 5240.1-R apply solely to this Classified Annex:

~~(S//SI)~~ Agent of a Foreign Power. For purposes of signals intelligence activities which are not regulated by the Foreign Intelligence Surveillance Act (FISA), the term "agent of a foreign power" means:

(a) a person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities, sabotage, or international terrorist activities, or activities in preparation for international terrorist activities, or who conspires with, or knowingly

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20291123~~

aids and abets such a person engaging in such activities;

(b) a person who is an officer or employee of a foreign power;

(c) a person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

(d) a person in contact with or acting in collaboration with an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has or has had access; or

(e) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power.

(U) Communicant. The term "communicant" means a sender or intended recipient of a communication.

(U) Consent. For the purposes of signals intelligence activities, an agreement by an organization with the National Security Agency to permit collection of information shall be deemed valid consent if given on behalf of such organization by an official or governing body determined by the General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

~~(S//SI)~~ Foreign Communication. The term "foreign communication" means a communication that involves a sender or an intended recipient who is outside the United States or that is entirely among foreign powers or between a foreign power and officials of a foreign power. Electronic surveillance within the United States targeted against communications entirely among foreign powers or between a foreign power and officials of a foreign power will be coordinated with the Federal Bureau of Investigation, including surveillances targeted against telephone communications or telecommunications that serve residential or non-official premises of a foreign power or foreign officials within the United States. This coordination is intended to satisfy the National Security Agency and the Federal Bureau of Investigation intelligence requirements, preclude duplication of effort, and ensure that appropriate minimization practices are developed and applied.

(U) Foreign Intelligence. The term "foreign intelligence" includes both positive foreign intelligence and counterintelligence.

~~(C)~~ Illicit Communication. The term "illicit communication" means a communication transmitted in violation of the Communications Act of 1934 and regulations thereunder or of international agreements which because of its explicit content, message characteristics, or

method of transmission is reasonably believed to be a communication to or from an agent or agents of foreign powers, whether or not United States persons.

(U) Interception. The term "interception" means the acquisition by the United States Signals Intelligence System through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligence form but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signal without reference to the information content carried by the signal.

~~(C)~~ International Commercial Communications. The term "international commercial Communications" means foreign communications transmitted internationally in whole or in part by one or more commercial or foreign government communications carriers, and includes, but is not limited to, [redacted] International commercial communications may be wire, telephone or radio communications transmitted by high frequency, microwave, satellite or other mode of transmission.

~~(C)~~ National Diplomatic Communications. The term "national diplomatic communications" includes all communications, regardless of the mode of transmission, transmitted by or to a foreign power and to which no United States person is a communicant. The official communications of an international organization composed of foreign governments are included in the meaning of this term, provided, however that the communications of official representatives of the United States are not included.

~~(C)~~ Selection. The term "selection," as applied to manual and mechanical processing activities, means the intentional insertion of a name, cable, TELEX, or other address and answer back or other alpha-numeric device into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

~~(C)~~ Selection Term. The term "selection term" means the composite of individual terms used to effect or defeat selection of particular communications for the purpose of interception. It comprises the entire term or series of terms so used, but not any segregable term contained herein. It applies to both mechanical and manual processing.

(U) Technical Data Base. The term "technical data base" means information retained for cryptanalytic or traffic analytic purposes.

[redacted]

~~(C)~~ United States Person. For purposes of intentionally collecting the communications of a particular person, the term "United States person," in addition to the meaning in the Appendix to DoD Regulation 5240.1-R, includes any alien known to be presently in the United States; any unincorporated association of such aliens or American citizens; the United States

operations, office, branch, or representative of a corporation incorporated abroad; any corporation or corporate subsidiary incorporated in the United States; and any U.S. flag non-governmental aircraft or vessel: Provided, however, that the term "U.S. person" shall not include (i) non-permanent resident aliens and entities in the United States that have diplomatic immunity as determined in accordance with Subsection 4.B; or (ii) a foreign power or powers as defined in Section 101 (a)(1)-(3) of FISA.

Sec. 3: Policy (U)

(U) The Director, National Security Agency, is assigned responsibility for signals intelligence collection and processing activities and communications security activities. In order to assure that these activities are conducted in accordance with the provisions of Executive Order 12333, the Director, or his designee, will issue appropriate directives and instructions implementing these procedures and governing the conduct of the United States Signals Intelligence System and the activities of communications security entities.

~~(C)~~ It is the policy of the United States Signals Intelligence System to collect, retain, and disseminate foreign communications and military tactical communications. It is recognized, however, that the United States Signals Intelligence System may incidentally intercept non-foreign communications, including those of or concerning United States persons, in the course of authorized collection of foreign communications. The United States Signals Intelligence System makes every reasonable effort, through surveys and technical means, to reduce to the maximum extent possible the number of such incidental intercepts acquired in the conduct of its operations. Information derived from these incidentally intercepted non-foreign communications may be disseminated to the Federal Bureau of Investigation when the information is foreign intelligence or counterintelligence or indicates a threat to the physical safety of any person. Dissemination of such information is also governed by these procedures and applicable minimization procedures approved in accordance with FISA. Specific communications sent from or intended for receipt by the United States persons are not intercepted deliberately by the United States Signals Intelligence System unless specific authorization for such interception has been obtained in accordance with these procedures.

~~(S//SI)~~ The President has authorized, and the Attorney General hereby specifically approves, interception by the United States Signals Intelligence System of:

* National Diplomatic Communications;

* International Commercial Communications;

* Illicit Communications;

* United States and Allied Military exercise communications;

* Signals collected during the search of the signals environment for foreign communications that may be developed into sources of signals intelligence;

* Signals collected during the monitoring of foreign electronic surveillance activities directed at United States communications consistent with the Foreign Intelligence Surveillance Act of 1978; and

* Signals collected during the testing and training of personnel in the use of signals intelligence collection equipment in the United States consistent with the Foreign Intelligence Surveillance Act of 1978.

Sec. 4: Procedures (U)

A. ~~(C)~~ Signals Intelligence: Communications of, or concerning, United States persons. The United States Signals Intelligence System may collect, process, retain and disseminate foreign communications that are also communications of, or concerning, United States persons. Communications of, or concerning, United States will be treated in the following manner.

1. Collection

(a) ~~(S//SI)~~ Communications of or concerning a United States person may be intercepted intentionally or selected deliberately through use of a selection term or otherwise only:

(1) with the consent of such United States person. Where a United States person has consented, by completion of the appropriate Consent Agreement appended hereto, to the use of a selection term intended to intercept communications originating by or referencing that person, the National Security Agency may use such selection term to select foreign communications; or

(2) with specific prior court order pursuant to the Foreign Intelligence Surveillance Act of 1978 where applicable. All United States Signals Intelligence System requests for such court orders or approvals shall be forwarded by the Director, National Security Agency for certification by the Secretary of Defense or the Deputy Secretary of Defense (in case of the unavailability of both of these officials and in emergency situations, certification may be granted by another official authorized by executive order to certify such requests), and thence to the Attorney General; or

(3) with the specific prior approval of the Director, National Security Agency, in any case in which the United States person is reasonably believed to be held captive by a foreign power or by a group engaged in international terrorist activities. The Attorney General will be notified when the Director authorizes selection of communications concerning a United States person pursuant to this provision; or

(4) with specific prior approval by the Attorney General based on a finding by the Attorney General that there is probable cause to believe the United States person is an agent of a foreign power and that the purpose of the interception or selection is to collect significant foreign intelligence. Such approvals shall be limited to a period of time not to exceed ninety days for individuals and one year for entities.

(b) ~~(S//SI)~~ Communications of, or concerning (1) [redacted] of a foreign power, or powers, as defined in Section 101 (a) (1) - (3) of FISA, or (2) [redacted] may be intercepted intentionally, or selected deliberately (through the use of a selection term or otherwise), upon certification in writing by the Director, NSA to the Attorney General. Such certification shall take the form of the Certification Notice appended hereto. An information copy shall be forwarded to the Deputy Secretary of Defense. Collection may commence upon the Director, NSA's certification. In addition, the Director, NSA shall advise the Attorney General and the Deputy Secretary of Defense on an annual basis of all such collection.

(c) ~~(C)~~ For purposes of the application of Parts 1, 2 and 3 of Procedure 5 (and subsection 4.A.1 (a) of this annex) to the activities of the United States Signals Intelligence System, any deliberate interception, selection or use of a selection term shall be deemed to constitute electronic surveillance; and "significant foreign intelligence" shall mean not only those items of information that are in themselves significant, but also items that are reasonably believed, based on the experience of the United States Signals Intelligence System, when analyzed together with other items, to make a contribution to the discovery of "significant foreign intelligence."

(d) ~~(S//SI)~~ Emergencies:

(1) The emergency provision in Section D of Part 2, Procedure 5, of DoD 5240.1-R, may be employed to authorize deliberate selection of communications of, or concerning, a United States persons defined in the Appendix to DoD Regulation 5240.1-R, when that person is outside the United States.

(2) If the United States Signals Intelligence System is intentionally collecting the communications of or concerning a non-resident alien abroad who enters the United States in circumstances that suggest that the alien is an agent of a foreign power, collection of the communications of that alien may continue for a period not to exceed seventy-two hours after it is learned that the alien is in the United States while the United States Signals Intelligence system seeks authority to continue the surveillance from the Attorney General pursuant to these procedures. [redacted]

[redacted] Communications acquired after the target is known to be in the United States, and that are not solely of, or concerning, U.S. citizens or permanent resident aliens, may be disseminated for foreign intelligence purposes until such time as diplomatic status is established or Attorney General approval is obtained. In those instances in which the diplomatic status of the alien is established, or Attorney General approval for continued surveillance is obtained, communications of, or concerning, the alien may be disseminated in accordance with subsection 4.A.4 of these procedures.

(3) If the United States Signals Intelligence System is intentionally collecting communications of, or concerning, a United States citizen or permanent resident alien abroad, it must terminate the surveillance promptly upon learning that person is in the United States. Electronic surveillance may be reinstituted only in accordance with FISA. In the event communications of, or concerning, the target continue to be collected before termination can be effected, processing and use of information derived from such communications shall be restricted to the greatest extent possible and special care shall be taken to ensure that such information is not disseminated for any purpose unless authorized in accordance with the provisions of FISA.

(e) ~~(S//SI)~~ Communications transmitted on [redacted] with a terminal in the United States that services a U.S. person may be targeted for interception upon certification in writing by the Director, NSA to the Attorney General that the target of the collection is a foreign entity and that the purpose of the collection is to obtain foreign intelligence. The certification shall take the form of the Certification Notice appended hereto. Collection may commence upon the Director, NSA's certification. In addition, the Director, NSA will advise the Attorney General on an annual basis of all such [redacted] collection. The Deputy Secretary of Defense will be provided information copies of all certifications sent to the Attorney General.

(f) ~~(S//SI)~~ Provided the proposed monitoring is not otherwise regulated by Section 4.A.1 (a)-(e), voice and facsimile communications with one communicant in the United States may be targeted for intercept only with the prior approval of the Attorney General or the Director, National Security Agency, as set forth below, unless those communications occur over channels used exclusively by a foreign power. The Director, National Security Agency, may approve the targeting of such communications if technical devices [redacted] are employed that limit acquisition by the National Security Agency to communications where the target is a non-U.S. person located outside the United States. [redacted] or to specific forms of communications used by those targets, [redacted] communications. In those cases in which it is not possible to use such technical devices, the Attorney General must approve the targeting. Approvals granted by the Director, NSA under this provision shall be available for review by the Attorney General.

(g) ~~(C)~~ [redacted] may be intercepted in accordance with Section 3 of this Annex.

(h) ~~(S//SI)~~ Use of direction finding solely to determine the location of a transmitter does not constitute electronic surveillance or collection even if directed at transmitters believed to be used by United States persons. Unless collection of the communications is otherwise authorized pursuant to this annex, the contents of communications to which a United States person is a party monitored in the course of direction finding shall be used solely to identify the transmitter.

2. Retention (U)

~~(S//SI)~~ Foreign communications of, or concerning, United States persons that are intercepted by the United States Signals Intelligence System may be retained in their original form or as transcribed only:

(a) if processed so as to eliminate any reference to United States persons;

(b) if necessary to the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future intelligent requirement. Sufficient duration may vary with the nature of the exploitation. In the context of a cryptanalytic effort, sufficient duration may consist of a period of time during which encrypted material is subject to, or of use in, cryptanalysis. In the case of international commercial communications that may contain the identity of United States persons and that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, National Security Agency, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or

(c) if dissemination of such communications without elimination of references to such United States persons would be permitted under section 4.A.4 below.

3. Processing (U)

(a) ~~(S//SI)~~ Foreign communications of, or concerning, United States persons must be processed in accordance with the following limitations:

(1) When a selection term is intended to intercept a communication on the basis of encipherment or some other aspect of the content of the communication, rather than the identity of a communicant or the fact that the communication mentions a particular individual:

(a) No selection term may be used that is based on content and that is reasonably likely to result in the interception of communications to or from a United States person, or which has in the past resulted in the interception of a significant number of such

communications, unless there is reasonable cause to believe that foreign intelligence or counterintelligence will be obtained by use of such a selection term.

(b) All such selection terms shall be reviewed annually by the Deputy Director for Operations, National Security Agency, or his designee to determine whether there is reasonable cause to believe that foreign intelligence or counterintelligence will be obtained by the use of these selection terms. The review of such selection terms shall include an examination of whether such selection terms have in the past resulted in the acquisition of foreign intelligence.

(c) Selection terms based on content that have resulted or that are reasonably likely to result in the interception of communications to or from a United States person shall be designed to defeat, to the extent practicable under the circumstances, the interception of such communications not containing foreign intelligence.

(2) Foreign communications collected by the United States Signals Intelligence System or other authorized entities may be forwarded to the National Security Agency as intercepted. This applies to forwarding to intermediate processing facilities, including those of authorized collaborating centers pursuant to written agreements, provided such forwarding does not result in the production by the United States Signals Intelligence System of information in violation of these procedures.

(b) ~~(S//SI)~~ Except as provided in (b)(1), radio communications that pass over channels with a terminal within the United States must be processed by use of selection terms, unless these communications occur over channels used exclusively by a foreign power.

(1) Radio communications that pass over channels with a terminal in the United States may be processed without the use of selection terms only when necessary to determine whether a channel contains communications of foreign intelligence interest which the National Security Agency wishes to collect. Processing under this section may not exceed two hours without approval of the Deputy Director for Operations, National Security Agency, and shall in any event be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include foreign intelligence. Once it is determined that the channel contains a sufficient amount of communications of foreign intelligence interest to warrant collection and exploitation to produce foreign intelligence, additional processing of the channel must utilize selection terms.

4. <u>Dissemination</u> (U)

~~(C//SI)~~ Dissemination of signals intelligence derived from foreign communications of, or concerning, United States persons is governed by Procedure 4 of DoD Regulation 5240.1-R. Dissemination of signals intelligence shall be limited to authorized signals intelligence consumers in accordance with requirements and tasking established pursuant to Executive Order 12333. Dissemination of information that is not pursuant to such requirements or tasking that

constitutes foreign intelligence or counterintelligence or that is otherwise authorized under Procedure 4 shall be limited to those departments or agencies that have subject matter responsibility. Dissemination of the identity of a United Stated person is authorized if it meets one of the following criteria, each of which is also deemed to meet the standard of "necessary to understand or assess" the importance of foreign intelligence information (otherwise, the identity of the United States person must be replaced by a generic term, e.g., United States citizen or United States corporation):

(a) The United States person has consented to the use of communications of or concerning him or her and has executed the applicable consent form;

(b) the information is available publicly;

(c) the identity of the United States person is that of a senior official in the Executive Branch. When this exemption is applied, the Deputy Director for Operations, National Security Agency, will ensure that domestic political or personal information is not retained or disseminated;

(d) the communication or information indicates that the United States person may be an agent of a foreign power;

(e) the communication or information indicates that the United States person may be:

(1) a foreign power as defined in Section 101 (a)(4) or (6) of FISA;

(2) residing outside the United States and holding an official position in the government or military forces of a foreign power such that information about his or her activities would constitute foreign intelligence;

(3) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

(4) acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to information or material classified by the United States;

(f) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(g) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information;

(h) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(i) the interception of the United States person's communications was authorized by a court order issued pursuant to Section 105 of FISA or by Attorney General approval issued pursuant to Section 4.A.1 of this annex and the communication may relate to the foreign intelligence or counterintelligence purpose of the surveillance;

(j) the communication or information indicates a possible threat to the safety of a person or organization, including those who are targets, victims, or hostages of international terrorist organizations;

(k) the communication or information indicates that the United States person may be engaged in international narcotics trafficking activities;

(l) the communication or information is evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes; or

(m) the identity of the United States person is otherwise necessary to understand foreign intelligence or counterintelligence or assess its importance. Access to technical data bases will be restricted to signals intelligence collection and analytic personnel. Requests for access from other personnel or entities shall be referred to the Deputy Director for Operations, National Security Agency. Domestic communications in which all communicants are United States persons shall be disposed of upon recognition, provided that technical data concerning frequency and channel usage may be retained for collection avoidance purposes.

B. ~~(C)~~ Signals Intelligence: Communications of, or Concerning, Aliens and Entities [redacted]. The United States Signals Intelligence System may intentionally intercept the international communications of non-permanent resident aliens and entities in the United States [redacted]

C. ~~(C)~~ Signals Intelligence: Illicit Communications. The United States Signals Intelligence System may collect, retain, process, and disseminate illicit communications without reference to the requirements concerning United States persons.

D. ~~(C)~~ Signals Intelligence: Search and Development. The United States Signals Intelligence System may conduct search and development activities with respect to signals throughout the radio spectrum under the following limitations:

1. Collection. Signals may be collected only for the purpose of identifying those signals that:

(a) may contain information related to the production of foreign intelligence or counterintelligence;

(b) are enciphered or appear to contain secret meaning;

(c) are necessary to ensure efficient signals intelligence collection or to avoid the collection of unwanted signals; or

(d) reveal vulnerability of United States communications security.

2. Retention and Processing. Communications originating or intended for receipt in the United States, or originated or intended for receipt by United States persons, shall be processed in accordance with Section 4.A.3, provided that information necessary for cataloging the constituent elements of the signal environment may be produced and retained if such information does not identify a United States person. Information revealing a United States communications security vulnerability may be retained.

3. Dissemination. Information necessary for cataloging the constituent elements of the signal environment may be disseminated to the extent such information does not identify United States persons, except that communication equipment nomenclature may be disseminated. Information that reveals a vulnerability of United States communications security may be dissemination to the appropriate security authorities.

E. ~~(S//SI)~~ Foreign Electronic Surveillance Activities. The United States Signals Intelligence System may collect information related to the conduct of electronic surveillance activities by foreign powers conducted within the United States against communications originated or intended for receipt in the United States. Collection efforts must be reasonably designed to intercept, or otherwise obtain only the results of such foreign surveillance efforts, and to avoid, to the extent feasible, the intercept of other communications. Such activities shall be conducted pursuant to orders of the United States Foreign Intelligence Surveillance Court.

F. (U) Assistance to the Federal Bureau of Investigation.

1. In accordance with the provisions of Section 2.6 (c) of E.O. 12333, the National Security Agency may provide specialized equipment and technical knowledge to the Federal Bureau of Investigation to assist the Bureau in the conduct of its lawful functions. When requesting such assistance, The Federal Bureau of Investigation shall certify to the General Counsel, National Security Agency, that such equipment or technical knowledge is necessary to accomplishment of one or more of the Bureau's lawful functions.

2. The National Security Agency may also provide expert personnel to assist Bureau personnel in the operation or installation of specialized equipment when that equipment is to be employed to collect foreign intelligence or counterintelligence. When requesting the assistance of expert personnel the Federal Bureau of Investigation shall certify to the General Counsel, National Security Agency, that such assistance is necessary to collect foreign intelligence or

counterintelligence and that the approval of the Attorney General (and when necessary an order from a court of competent jurisdiction) has been obtained.

//s//
William R. Taft
DEPUTY SECRETARY OF DEFENSE
26 April 1988

//s//
Edwin Meese III
ATTORNEY GENERAL
27 May 1988

Executive Order 12333
Consent Agreement
Signals Intelligence Coverage

I. ____________(full name)____________, ____________title__________, hereby consent to the National Security Agency undertaking to seek and disseminate communications to or from or referencing me in foreign communications for the purpose of __________________.

This consent applies to administrative messages alerting elements of the United States Signals intelligence System to this consent as well as to any signals intelligence reports which may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12333 procedures, this consent covers only information which relates to the purpose stated above and is effective for the period:

__________________.

Signals intelligence reports containing information derived from communication to or from me may only be disseminated to me and to ____________. Signals intelligence reports containing information derived from communication referencing me may only be disseminated to me and to [names of departments and agencies, e.g., DoD, CIA, etc] except as otherwise permitted by procedures under Executive Order 12333.

(SIGNATURE)
(TITLE)

(UNCLASSIFIED until completed. Classify completed form based on information added, but not lower than CONFIDENTIAL.)

Executive Order 12333
Consent Agreement
Signals Intelligence Coverage

I. ____________(full name)____________, ____________title__________, herby consent to the National Security Agency undertaking to seek and disseminate references to me in foreign communications for the purpose of __________________.

This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent as well as to any signals intelligence reports which may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12333 procedures, this consent covers only references to me in foreign communications and information derived therefrom which relates to the purpose stated above. This consent is effective for the period:

________________.

Signals intelligence reports containing information derived from communications referencing me and related to the purpose stated above may only be disseminated to me and to [names of departments and agencies, e.g., DoD, CIA. etc] except as otherwise permitted by procedures under Executive Order 12333.

(SIGNATURE)
(TITLE)

(UNCLASSIFIED until completed. Classify completed form based on information added, but not lower than CONFIDENTIAL.)

[redacted]

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

Publicly available - goes to end of this doc

JUN 17 2009

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 08-052 – DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters

References: See Attachment 1

Purpose. This DTM implements recent Executive Branch guidance in Director of National Intelligence and Chairman, Intelligence Oversight Board Memorandum (Reference (a)) concerning the criteria and requirements for reporting intelligence oversight matters and directs compliance with the guidance contained in Attachment 2. It establishes the procedures to ensure complete and standardized reporting by the DoD Intelligence Components and other entities involved in intelligence activities, which include both foreign intelligence and counterintelligence activities. This DTM is effective immediately; it shall be incorporated into DoD 5240.1-R (Reference (b)) within 180 days. Nothing in this DTM is intended to alter reporting requirements established by statute or departmental policy.

Applicability. This DTM applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies,

the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

Policy. Questionable intelligence activities and significant or highly sensitive matters involving intelligence activities may have serious implications for the execution of DoD missions. It is DoD policy that senior leaders and policymakers within the Government be made aware of events that may erode the public trust in the conduct of DoD intelligence operations. Reference (b), DoD Directive 5148.11 (Reference (c)), and Executive Order (E.O.) 13462 (Reference (d)) require that such matters be reported to the Intelligence Oversight Board (IOB), a component of the President's Intelligence Advisory Board, and the Director of National Intelligence (DNI) as appropriate. The Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) is the principal staff assistant for intelligence oversight matters and shall serve as the conduit for all reporting to the IOB.

Reporting Requirements and Procedures. Reporting guidance is contained in Attachment 2. The quarterly report to the ATSD(IO) is exempt from licensing in accordance with Chapter 4, subparagraphs C4.4.1 and C4.4.8, of DoD 8910.1-M (Reference (e)).

Releasability. UNLIMITED. This DTM is approved for public release and is available on the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

Attachments:
As stated

ATTACHMENT 1

REFERENCES

(a) Director of National Intelligence and Chairman, Intelligence Oversight Board Memorandum, "Intelligence Oversight Reporting Criteria," July 17, 2008[1]
(b) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982
(c) DoD Directive 5148.11, "Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))," May 21, 2004
(d) Executive Order 13462, "President's Intelligence Advisory Board and Intelligence Oversight Board," February 29, 2008
(e) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
(f) Executive Order 12333, "United States Intelligence Activities," as amended
(g) Department of Justice-DoD Memorandum of Understanding: "Reporting of Information Concerning Federal Crimes," August 1995[2]

[1] Available at: http://www.defenselink.mil/atsdio
[2] Contact ATSD(IO), 703-275-6550

ATTACHMENT 2

PROCEDURES FOR REPORTING QUESTIONABLE INTELLIGENCE ACTIVITIES AND SIGNIFICANT OR HIGHLY SENSITIVE MATTERS

1. REPORTING PARAMETERS

a. The DoD Components shall report the following matters to the ATSD(IO) in accordance with References (a) and (d).

(1) Questionable Intelligence Activity. An intelligence activity, as defined in E.O. 12333 (Reference (f)), that may be unlawful or contrary to executive order, Presidential directive, or applicable DoD policy governing that activity.

(2) Significant or Highly Sensitive Matters. A development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity. Such matters might be manifested in or by an activity:

(a) Involving congressional inquiries or investigations.

(b) That may result in adverse media coverage.

(c) That may impact on foreign relations or foreign partners.

(d) Related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method. Reporting under this paragraph does not include reporting of routine security violations.

(3) Crimes Reported to the Attorney General. Any intelligence activity that has been or will be reported to the Attorney General, or that must be reported to the Attorney General as required by law or other directive, including crimes reported to the Attorney General as required by Department of Justice-DoD Memorandum of Understanding (Reference (g)).

b. Unless extenuating circumstances exist, the ATSD(IO) will be notified prior to briefings of any congressional committee or member of Congress concerning intelligence matters identified in paragraphs 1.a.(1), 1.a.(2), and 1.a.(3) of this attachment. Should extenuating circumstances, in fact, delay notification to the ATSD(IO) until after the briefing, then the ATSD(IO) will be notified of the outcome of the briefing at the first opportunity thereafter.

c. The DoD Component assigned to or conducting intelligence activities may establish internal organizational reporting responsibilities pursuant to that Component's internal policies and regulations.

2. <u>SUBMISSION OF REPORTS</u>. DoD Components assigned to conduct intelligence and counterintelligence activities shall submit reports to the ATSD(IO) in accordance with the following guidance.

a. Report questionable intelligence activities of a serious nature and all significant or highly sensitive matters immediately. Such reports may be made by any secure means. Oral reports should be documented with a written report as soon as possible thereafter.

b. Report questionable intelligence activities not of a serious nature quarterly. Reporting periods shall be based on the calendar year. The first report for each calendar year shall cover January 1 through March 31. Succeeding reports shall follow at 3-month intervals. Quarterly reports are due to the ATSD(IO) by the 15th day of the month following the end of the quarter. Quarterly reports will describe all questionable intelligence activities as well as significant or highly sensitive matters identified during the quarter. Quarterly reports are routinely submitted to the ATSD(IO) through normal modes of routing and transmission (e.g., chain of command, hard or soft copy). Quarterly reports are required even if no reportable matters occurred during the reporting period.

c. Reporting DoD Components will format all reports as follows:

(1) <u>Assignment of a Case Number for Each Incident</u>. Except where the volume of incident investigations that have been reported and closed within the same reporting quarter makes the assigning of a case number to each case impracticable, a case number that runs consecutively and identifies the reported incident by reporting agency, Military Department, or Combatant Command and calendar year shall be assigned to each incident. For example: "DIA 2009 - 04" would indicate the fourth incident reported by DIA in calendar year 2009. Use this number each time the incident is mentioned in initial reports, and in update and close-out reports. A case number will be assigned to all reported incidents that, at a minimum, are the subject of an ongoing investigation.

(2) <u>Information to be Included in Each Report</u>. For each incident reported, include the following information as it becomes available.

(a) A narrative describing each incident reported.

(b) An explanation of why the incident is being reported either as a potential violation of law, potentially contrary to executive order or Presidential directive, or a potential violation of Reference (b) and/or agency or Military Department procedures implementing Reference (f). Cite the portions of relevant law, order, policy, or regulation as it is determined.

(c) An explanation of why the incident is considered a significant or highly sensitive matter, if so reported.

(d) An analysis of how or why the incident occurred.

(e) An assessment of the anticipated impact of the reported incident on national security or international relations, as well as any mitigation efforts, including success and failures of such efforts. If there has been no impact or no impact is anticipated, the report should so state.

(f) Remedial action taken or planned to prevent recurrence of the incident.

(g) An assessment of any impact the reported incident may have on civil liberties or protected privacy rights.

(h) A description of actions taken if the incident concerns information improperly acquired, handled, used, or destroyed.

(i) Any additional information considered relevant for purposes of fully informing the Secretary and/or Deputy Secretary of Defense, the IOB, and the DNI and providing context about the incident.

d. Each quarterly report should be organized under the major headings of "New Incidents" and "Updates on Previously Reported Incidents." The latter heading includes incidents still under inquiry as well as those resolved and closed during the quarter.

e. Additionally, each quarterly report will contain a summary of gravity, frequency, trends and patterns of the questionable intelligence activities, and/or significant or highly sensitive incidents reported during that quarter, to the extent that they can be determined. Otherwise, the summary should be provided, as the information becomes available, in a subsequent quarterly report.

f. The quarterly report shall include a description of any inspection findings or intelligence oversight program developments, such as publication of a revised intelligence oversight regulation, that the reporting DoD Component believes is significant. Neither training reports nor inspection schedules shall be included in the

quarterly report to ATSD(IO). DoD Components shall monitor compliance with training requirements and inspection schedules.

g. Reporting shall not be delayed or postponed pending an investigation, command inquiry, or legal proceeding.

3. PROHIBITED USE OF THIS ATTACHMENT. This attachment shall not be used to prepare the Annual Intelligence Oversight Report to Congress, which is signed by the Secretary of Defense. Instructions for preparing the Annual Intelligence Oversight Report to Congress will be issued by the ATSD(IO) in November of each year; the Annual Report will be due to the ATSD(IO) January 31 of each year.